IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 19 February 2023, accepted 16 March 2023, date of publication 22 March 2023, date of current version 29 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3260777

RESEARCH ARTICLE

A Promising Integration of SDN and Blockchain for IoT Networks: A Survey

STEPHEN W. TURNER[1], (Member, IEEE), MURAT KARAKUS[2], EVRIM GULER[3], AND SULEYMAN ULUDAG[1], (Member, IEEE)

[1]Department of Computer Science, University of Michigan-Flint, Flint, MI 48502, USA
[2]Department of Software Engineering, Ankara University, 06100 Ankara, Turkey
[3]Department of Computer Engineering, Bartin University, 74100 Bartin, Turkey

Corresponding author: Stephen W. Turner (swturner@umich.edu)

This work was supported by the Scientific & Technological Research Council of Turkey (TUBITAK) under Grant 120E448.

ABSTRACT The state of computer network technologies has continually advanced at a rapid pace. Software Defined Networking (SDN) and Blockchain (BC) have emerged as complementary technologies providing support that facilitates greater security and greater network performance for many domains of application, including the Internet of Things (IoT) ecosystem, ideally resulting in an improvement to our collective quality of life. The proliferation of IoT devices is driven by a wide variety of use cases and by their ubiquitous availability. When combined with the emergence of SDN and BC, this environment presents rich opportunities for various emerging research efforts and provides a motivation for this paper. Here, we present a comprehensive survey of the studies in which BC and SDN have been integrated into the IoT ecosystem, referred to hereafter as BC-enabled Software-Defined IoT (BC-SDIoT). The paper first discusses the motivations and drivers for integrating BC-enabled SDN and BC-SDIoT, as well as their benefits and drawbacks. Second, we categorize the relevant studies according to six key implementation objectives and ideas that combine BC, SDN, and IoT technologies to create smart, secure, and effective frameworks: Security, computing paradigms (edge and fog computing), trust management, access control & authentication, privacy, and networking. In the corresponding sections, we present the categories (i.e., problem domains) of the aforementioned novel taxonomy and discuss related studies (i.e., solutions) in depth. Finally, we outline potential major challenges, open issues, and future prospects that require further research attention and intensive endeavors for complete and ground-breaking frameworks to broaden newer research domains in BC-SDIoT. This survey paper may serve as a fruitful primer for the reader investigating the exploitation of BC in SDN and IoT ecosystems.

INDEX TERMS Blockchain, IoT, SDN, survey, BC-SDIoT.

I. INTRODUCTION

As our needs for improved network services have increased, we have collectively observed the technologies of computer networks advancing quickly to keep up with our society's demands. The operational needs of devices, along with the constraints imposed by network connectivity, have changed rapidly in recent years. Two notable developments have received expanded interest among the research communities: the emergence of Software Defined Networking (SDN) [1] and Blockchain (BC) [2] provide many opportunities for secure and flexible network management, which are important characteristics in the rapidly growing domain of the Internet of Things (IoT) [3]. These technologies can be implemented in numerous different contexts, each with its own advantages and disadvantages.

The associate editor coordinating the review of this manuscript and approving it for publication was Jad Nasreddine.

A. PRELIMINARIES

As is evident in the expanding worldwide deployments, SDN and BC have emerged as complementary technologies

that provide support for ensuring security while improving network performance. According to Statista,[1] the worldwide market sizes of SDN, BC, and IoT are growing rapidly. In 2020, the market size of SDN was $8B and is projected to reach $43.3B by 2027, with a compound annual growth rate of 19%.[2] As shown in Fig. 1, the worldwide market size of BC is nearly $12B in 2022, with a projected value of nearly $163B by 2027.[3] Meanwhile, the global market for the IoT is already significantly larger, with market size of $749B in 2020 and projected to reach $1.1Tr in 2023.[4] This mirrors the growth in the number of IoT devices worldwide, which is nearly 43B in 2022 and projected to grow to nearly 76B in 2025[5] as shown in Fig. 2.

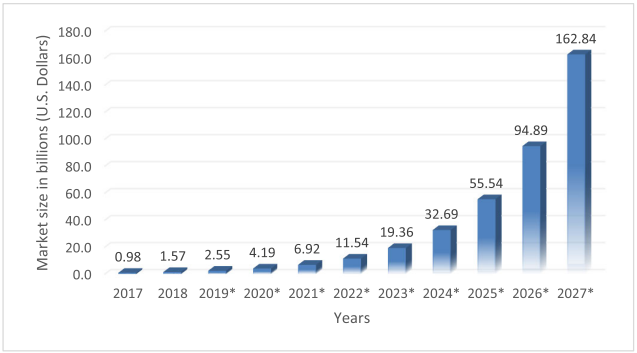


FIGURE 1. Size of the blockchain technology market worldwide from 2017 to 2027.[3]

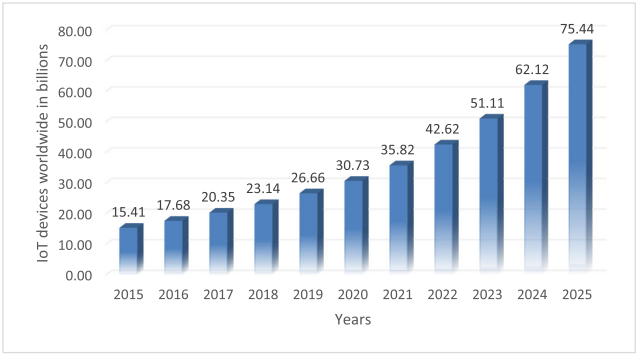


FIGURE 2. Number of IoT devices worldwide from 2015 to 2025 in billions.[5]

This growth is being driven by a wide variety of newly discovered use cases. The applications of IoT are numerous, and the technology has become ubiquitous due to its capabilities for improving the devices that we use in our everyday lives. SDN is the most important breakthrough of the past two decades in computer networking, enabling more effective and flexible network management, which in turn improves the performance of the network in support of other technologies like BC and IoT. Since the invention of BC, organizations worldwide have begun to employ it in numerous areas. Among the most commonly cited use cases, BC is employed in digital currency, secure information exchange, asset tracking and management, digital identification, regulatory compliance, financial flow traceability, digitization of documents and records, licensing/credentialing, tokenization of assets, tracking supply chains, payment/trading processing, contract management, internal control, and anti-counterfeiting.[6] The various use cases in organizations worldwide, as of 2021, are illustrated in Fig. 3.

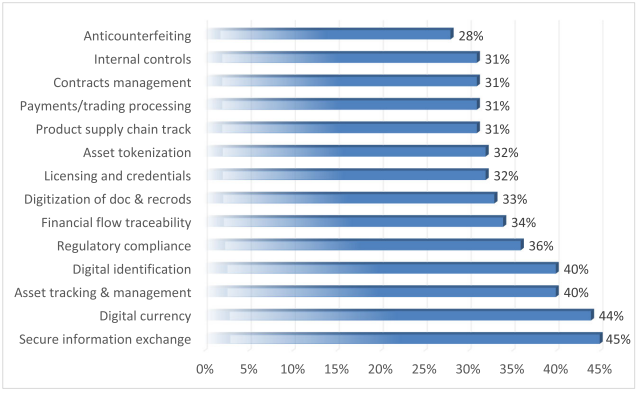


FIGURE 3. Blockchain technology use cases in organizations worldwide as of 2021 from Deloitte's 2021 Global Blockchain Survey [4] and also from the Statista report.[6]

SDN separates the control and data planes where network intelligence and state are logically centralized and the underlying network infrastructure is abstracted from the applications. BC is a decentralized database of transactions across a peer-to-peer network, where information is stored in encrypted blocks and tracked using ledgers stored on each network node. IoT is a significant driver of industrialized cyber-physical systems (CPSs). It has begun to engage in nearly every aspect of our daily lives, including monetary transactions, medicine, communication, security, the military, and home automation.

There are numerous motivations to study the integration of BC with SDN and IoT (*BC-SDIoT*). To start, IoT devices are inherently simple and lacking in security features [5]. As they become more common, it is only a matter of time before widespread security attacks occur to violate personal privacy, data integrity, etc. [5], [6], [7]. Simultaneously, BC is highly useful in securing some aspects of computer networks [8], [9], presenting a countermeasure opportunity for the defense of IoT networks. Coupled with

[1] https://www.statista.com

[2] https://www.statista.com/statistics/468636/global-sdn-market-size/

[3] https://www.statista.com/statistics/1015362/worldwide-blockchain-technology-market-size/

[4] https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/

[5] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[6] https://www.statista.com/statistics/878732/worldwide-use-cases-blockchain-technology/

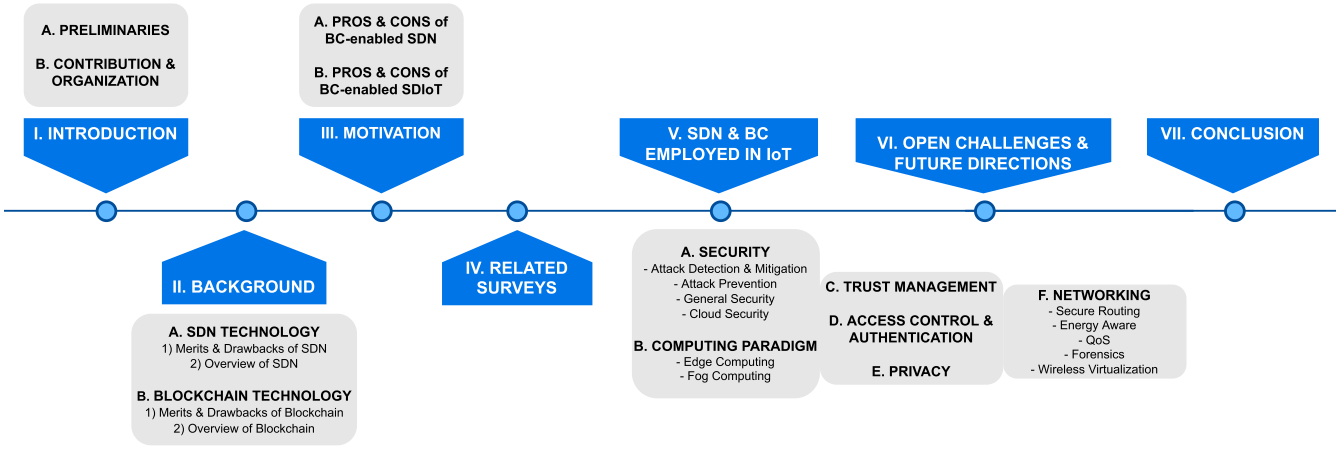


FIGURE 4. The outline of the paper structure.

its decentralized implementation, BC improves upon the single point of failure characteristic of shared digital assets. SDN is a technology that is highly useful in enabling flexible network management to optimize the Network Operations (NetOps) [1]. Accordingly, it becomes apparent that the combination of BC and SDN provides numerous opportunities to secure the IoT domain while effectively supporting the IoT infrastructure through better network control and management.

B. CONTRIBUTION AND ORGANIZATION

This paper presents a survey on the research efforts in which BC and SDN have been integrated into the IoT ecosystem (BC-SDIoT). Therefore, the scope of the study revolves around integrating three concepts: BC, SDN, and IoT. In this context, we organize the related studies into six categories that are the most prominent implementation goals and concepts in which BC, SDN, and IoT technologies amalgamate to provide intelligent, secure, and efficient frameworks: Security, computing paradigms, trust management, access control & authentication, privacy, and networking. It is worth noting that each of these categories reflects a problem domain in BC-SDIoT. Accordingly, the organization is a taxonomy of the problem domains therein. We explain these categories (i.e., problem domains) and related studies (i.e., solutions) in corresponding sections. Also, we give the motivations behind the integration of BC-enabled SDN and BC-SDIoT, along with the advantages and disadvantages. Finally, we outline the potential challenges, open problems, and future directions that should be addressed further, to develop breakthrough and comprehensive frameworks in BC-SDIoT networks. This survey paper may be a useful primer for a reader investigating the exploitation of BC in SDN and IoT ecosystems.

The following questions constitute the backbone and motivation for our investigation of the research works in BC-SDIoT:

Q1. What are the advantages and challenges of combining BC and SDN for IoT (BC-SDIoT) networks? (Section III)
Q2. What are the classifications of BC-SDIoT networks from the perspective of their implementation goals and respective research challenges regarding infrastructure, security, trust management, and data management? (Section V)
Q3. What are the open research challenges and potential future directions of BC-SDIoT networks in terms of infrastructure, security, trust management, and data management? (Section VI)

Answering the questions above, our main contributions are as follows:

- We provide overviews of BC and SDN technologies along with their merits and drawbacks.
- We introduce a novel taxonomy of approaches combining BC and SDN.
- We present a comprehensive discussion of existing studies that integrate the development and deployment of BC and SDN to serve an IoT infrastructure.
- We report on the status of existing open challenges, identifying new open challenges and potential research directions for SDN integrated with BC for IoT applications.

The outline of our paper's structure is as depicted in Fig. 4 and briefly explained as follows: Section II briefly explain SDN and BC technologies along with their merits and drawbacks as background information to make our paper as self-contained as possible. Section III elaborates on the advantages and disadvantages, as well as introducing a taxonomy of approaches, to the integration of BC with SDN. Section IV presents other survey papers of BC with various networking technologies, including SDN and IoT. Section V is an in-depth survey of the use of BC and SDN in the IoT ecosystem, together with the two novel classifications. A detailed discussion of open issues, challenges, and potential research directions is presented in Section VI. Finally, we provide the concluding remarks in Section VII.

II. BACKGROUND

Although SDN and BC technologies have great advantages, the widespread implementation of each is plagued by challenges such as integration, interoperability, adaptability, hybridization, processing of diversified data volume and types, etc. In this section, we give background information on SDN and BC technologies, presenting a discussion of their merits and drawbacks, as well as providing a technical overview of each, to make the paper self-contained.

A. SOFTWARE DEFINED NETWORKING (SDN) TECHNOLOGY

This section presents a brief overview of SDN, followed by a discussion of the benefits and disadvantages that SDN technology brings to networking architectures.

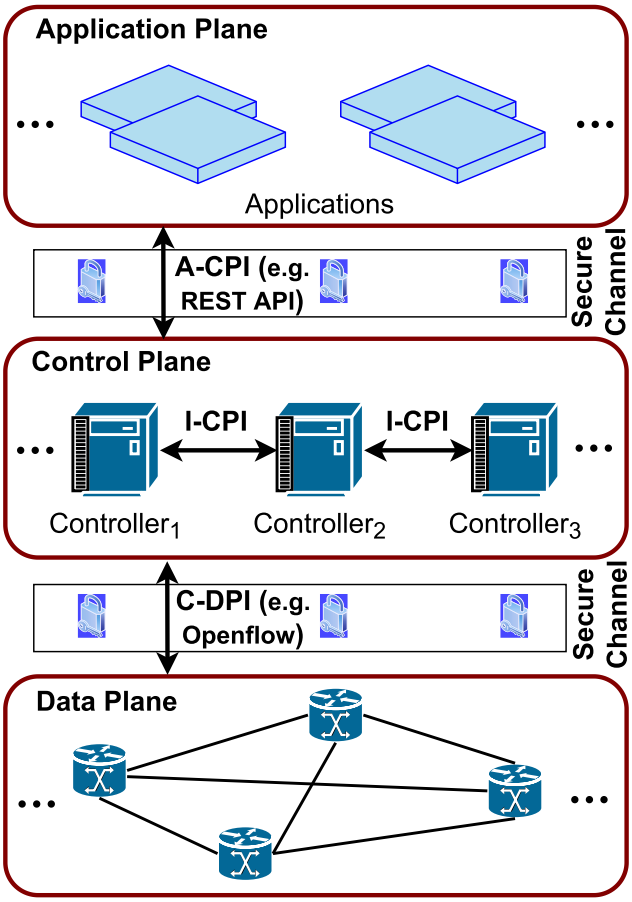


FIGURE 5. SDN architecture with its main planes and interfaces.

1) OVERVIEW OF SDN

The basic SDN architecture is mainly defined in three parts: Data plane, control plane, and application plane, as depicted in Fig. 5. SDN has interfaces between devices in a control plane and a data plane. These interfaces let devices communicate with others in the network. East-West APIs [10] aim to exchange information between controllers, which may be from the same or different organizations. Northbound APIs facilitate communication between network applications/services and controller(s), for purposes of network security, management, etc. In contrast, southbound APIs enable the communication between the controller(s) and data plane devices such as routers, physical switches, or virtual switches [11], [12], [13]. The OpenFlow [14], [15], [16], [17] protocol is the most prevalent standard southbound interface used for communication between the control and data planes [18]. SDN also simplifies network operations and reduces the cost of network administration. These advantages are provided via its programmable, centralized, vendor-free, and adaptable characteristics.

a: DATA PLANE

The data layer is comprised of networking equipment (e.g. routers, physical/virtual switches, and access points). Packet forwarding is a fundamental operation of the data layer. An SDN controller may contact and administer this equipment using Controller-Data Plane Interfaces (C-DPIs). C-DPI messages are sent within a secure channel, such as TLS. The OpenFlow protocol is the most widespread standard C-DPI used for connectivity among controller(s) and data layer equipment.

b: CONTROL PLANE

An SDN control layer may include one or more software-based SDN controllers. They deliver control functions by focusing on how the network forwards traffic using the C-DPI. In addition to the C-DPI, there are interfaces allowing interaction among controllers (Intermediate-Controller Plane Interface or I-CPI [10]) and between controllers and applications (Application-Controller Plane Interface or A-CPI). I-CPIs are exploited to share data among controllers. An A-CPI enables communication among network applications and controller(s) to communicate for security, management, etc. Functional components and control logic are the two primary components of a controller.

c: APPLICATION PLANE

An SDN application layer is comprised of applications that interact with the controller(s) and use an abstract view of the network in their interior decision-making algorithms to fulfill a particular networking task. These programs connect with the controller(s) over an open A-CPI interface, such as REST API. An SDN application is composed of an SDN App Logic and an A-CPI Driver. They are typically grouped based on the network services they accomplish, such as security, traffic engineering, load balancing, etc.

2) MERITS AND DRAWBACKS OF SDN

The architecture of conventional IP-based systems has surpassed its limits. Expanding cloud solutions, server virtualization, the dramatic rise of mobility, and data, such

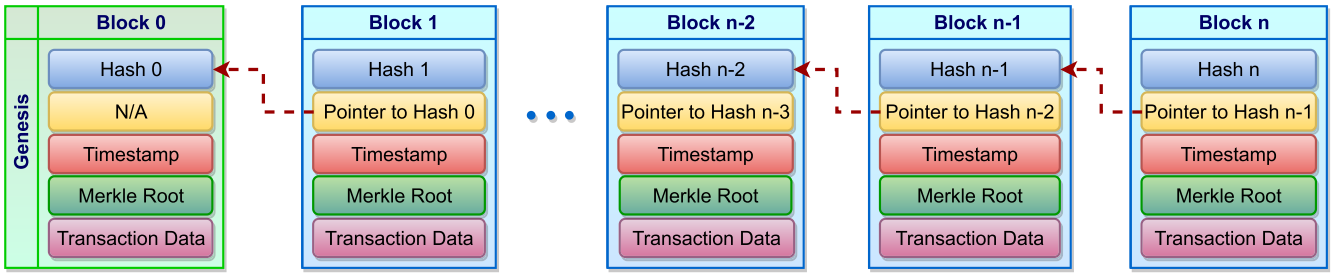


FIGURE 6. Overview of blockchain and block data structures.

as video and big data, have prompted experts to reconsider the network designs of today. In conventional topologies, network equipment is complicated, complex to (re)configure and (re)install, and requires qualified expertise. Adding or removing a node from a system incurs additional expense. IT personnel must work with many switches, routers, and other network hardware, as well as be able to update ACLs, VLANs, and several other techniques [19]. Moreover, when industry expectations or customer requirements expand daily, software developers, providers, and companies must engage in the introduction of new services and capabilities. Yet, companies' reliance on vendors is a hindrance that prevents them from creating new network apps and systems for their networks, given the lengthy production run of network hardware. Consequently, the data centers, providers, and organizations of today require more responsive network designs.

The SDN architecture [1], [20], [21], [22] has been developed as an answer to the constraints imposed by conventional networks. The goal of SDN is to separate the forwarding and control planes, which facilitates an effective allocation of network resources and enables programmability to alter system properties more effectively and more quickly. This makes network administration more convenient, simpler, and more cost-efficient since the separation allows network operators to swiftly administer, operate, and optimize network capacity using reactive, autonomous, and proprietary-free applications that they have created themselves under SDN [23]. Moreover, since network control is centralized in SDN, controllers have a holistic view and awareness of the entire network, as opposed to the view within traditional networking. Therefore, they can enhance resource utilization and flow management in response to network dynamics and contingencies.

SDN also presents several technical challenges. Sezer et al. [19] state that these challenges can be classified into four categories. The first is dealing with high-performance packet processing in a flexible/programmable manner. The second is interoperability or standardization, which needs to be addressed in the SDN infrastructure. The third is the security issues in SDN. The final category is its scalability, which needs more attention by researchers [24].

B. BLOCKCHAIN (BC) TECHNOLOGY

In this section, we first present an overview, followed by a discussion of the merits and drawbacks of BC technology in networking architectures.

1) OVERVIEW OF BC

BC is an update-only database that typically stores data that is small in size, usually records of transactions in a system. These records are individually encrypted to preserve security and anonymity, and all network nodes participating in a BC agree on the validity of each record, ensuring unanimous agreement on outcomes, and also establishing trust.

When a transaction occurs, it is added to the distributed database through specific steps: (i) a user executing a transaction submits it to the blockchain by using a private key to sign the transaction, broadcasting that to one-hop peers; (ii) the neighboring peers validate the incoming transaction then relay it such that the transaction eventually spreads across the entire network; (iii) after a (typically) agreed-upon time interval, nodes engage in a process that includes mining, involving processing overhead to create/propose a new block for validation, as well as participation in a consensus algorithm to validate the block; (iv) the block is added to the existing BC. Nodes may receive a *reward* for activities in the mining and consensus process, and the choice of mining nodes may depend on the consensus mechanism employed in the network.

The peer-to-peer nature of BC is an essential property that eliminates the need for a trusted third party and hence provides a solution to the well-known single-point-of-failure problem of centralized systems, including SDN. In systems with multiple equal participants, establishing trust is a known problem toward ensuring all participants can mutually agree on some solutions. BC uses consensus algorithms to ensure trust and alleviate the need for external authority. Consensus algorithms consume resources (e.g., CPU time), so a reward mechanism may be employed to incentivize participation. A *punishment* may also be used as a cost a node must pay if it violates a procedure, in order to discourage malicious behavior.

A high-level representation of the BC structure is illustrated in Fig. 6. Each block typically contains a sequence number, a hash, a pointer to a prior block using the prior

TABLE 1. Works citing specific blockchain advantages.

BC Advantages	Proposals
Immutability	[26]–[52]
Traceability	[28], [30]–[32], [35], [37], [42], [45], [47], [48], [53], [54]
Transparency	[28], [30]–[32], [34]–[38], [51], [52], [54]–[57]
Decentralization	[26], [28]–[30], [33], [35], [37]–[48], [51]–[53], [56]–[65]
Anonymity	[33], [34], [36], [37], [49], [64], [66]
Shared Ledger	[27], [35], [57], [65]
Trust-free	[27], [33], [37], [38], [49], [54]–[56], [58], [59], [66]

TABLE 2. Works citing specific blockchain disadvantages.

BC Disadvantages	Proposals
Computational Load	[29], [31]–[35], [41], [44], [45], [48], [55]–[57], [60], [65], [67]
Storage	[30], [38], [40]–[42], [44], [45], [48], [55], [60], [67]
Ledger Update Latency	[28], [33]–[35], [41], [42], [45], [48], [52], [56], [57], [60], [67]

block's hash, a timestamp, and a set of transaction data, for which it is desirable to maintain an immutable and secure record. The hash pointer data ensures a block's location in the chain, and the local hash is typically the hash of a Merkle tree root used to validate the information contained in the transactions stored in the block.

Several variations of blockchain exist, a classification of which is presented in [2]. The original version is a *public blockchain*, an open platform that allows anyone to join, transact, and mine. It is also known as *permissionless* because no access restrictions exist and all participants are given authority to read and write transactions. *Private blockchains* (also called *permissioned*) were developed to allow private sharing and exchange of data, with mining controlled by selected hosts (e.g. an organization), and access is restricted to specific entities. A hybrid approach is the *consortium blockchain*, which is partially private and partially public; a set of predetermined nodes are responsible for validating blocks and consensus, and they decide which nodes may belong to the network and which nodes may mine.

2) MERITS AND DRAWBACKS OF BC

BC has been developed in part from a desire to address the double-spending problem in cryptocurrency systems while simultaneously alleviating the need for a (single-point-of-failure) trusted third-party to store transaction records [25]. Since its inception, the applications of BC have expanded well beyond that of cryptocurrency, although that likely remains its most commonly publicized and known use case. BC's growing popularity in research and industrial circles is largely due to its positive characteristics or advantages.

Table 1 indicates how the works surveyed here specifically address one or more of the various advantages of the use of BC technology in their research. These advantages include:

- Immutability, the property that transactions cannot be changed once they are committed to the BC.
- Traceability, the property that the entire database is open and the history of transactions is completely available to be examined.
- Transparency, the property that transactions in a BC are publicly viewable due to its being stored at all participating hosts.
- Decentralization, the property that no centralized authority controls the BC.
- Anonymity, the property that transactions can be stored while preserving, yet hiding, the identity of those enacting the transactions.
- Shared ledger, the property that all nodes involved in the BC maintain an identical copy of it, which may also be referred to as unanimity.
- Trust, the property that allows mutually unknown or untrusting hosts to establish a trusting relationship, which is supported by BC technology.

Disadvantages identified previously include BC's requirement of computational load, storage, and latency. These are highlighted in Table 2, which identifies the works surveyed here that specifically address one or more of the various disadvantages of the use of BC technology in their research. Computational load is typically cited as a disadvantage due to the additional processing requirements of consensus algorithms, such as proof of work [25]. Storage is a disadvantage because each node participating in the BC stores an entire copy of the BC. Latency is a concern due to the computational requirements of various consensus algorithms, which slows the performance of BC implementations. Taken collectively, these disadvantages have raised concerns about the scalability of BC while simultaneously presenting opportunities for research efforts. The advantages and disadvantages of BC have been highlighted in Tables 1 and 2 in order to provide further guidance for researchers interested in refining their search with these specific characteristics.

III. MOTIVATION

The combination of technologies resulting in BC-SDIoT also has a number of advantage and disadvantages. The following subsections provide an elaboration on this statement by highlighting them, as well as introducing a taxonomy of approaches to the integration of BC with SDN.

A. PROS AND CONS OF BC-ENABLED SDN

The BC and SDN technologies are complementary and synergistic in the sense that they typically serve different purposes and can be combined to create a whole greater than the sum of parts. As noted in Section II-B, BC is, by design, a distributed database implementation in which transactions (or decisions) are transparently available and visible to all participants. In contrast, and as noted in Section II-A2, SDN is a technology employed to flexibly manage and

control operations in a network by separating network control from the data flows. The original conception of an SDN employs a single centralized controller with domain over an entire network, which represents a significant challenge in the form of performance scalability, as well as the issue of it becoming a single point of failure and a magnet for security attacks. A significant advantage of integrating BC with SDN is that the BC mitigates the problem of having a single point of failure by enabling a network of SDN controllers to collaborate and collectively make decisions that are mutually trustworthy and immutable. This allows security measures to be integrated into BC-SDN implementations, and it facilitates scaling of the network infrastructure as needed.

Additionally, some of the challenges of BC are addressed through its combination with SDN. Computational load is often cited as a problem with BC implementations, and several works surveyed here examine consensus algorithms requiring lower computational effort. However, it is also true that SDN controllers are typically fully equipped computers with high-powered CPUs and sufficient memory to execute the consensus algorithms required by BC. These characteristics enable them to store the BC and to execute with sufficient speed so as to reduce compute (clock) time as much as poassible. We also note that consortium and private BC implementations may require a lighter computational load, as reflected in some of the papers cited in this survey.

The examination of the literature revealed a taxonomy of three primary approaches in the implementation of a BC-enabled SDN, as illustrated in Fig. 7:

1) *Integrated approach*, in which the BC is implemented directly as an integral part of each SDN controller. Typically, the BC plays a key role in implementing algorithms executed in the control or data planes of the SDN controller, albeit more often in the control plane. For example, BC may be used to establish a consensus among SDN controllers concerning flow rules updates.
2) *Collaborative/cooperative approach*, in which the BC and the SDN are separated but work together to accomplish a single goal. The BC isn't implemented as a part of the SDN control stack but may provide some service, to assist the SDN controller in its functions. For example, SDN controllers may employ BC as a service to be consulted in making flow rule updates.
3) *Overlay approach*, in which the BC is implemented alongside the SDN but does not directly provide input into the SDN's operations. Working separately, the SDN continues its usual management and control functions, while the BC is added to provide an additional service, such as security. For example, the SDN may focus on network control, while the BC as an overlay provides separate security services.

Table 3 presents a classification of the literature surveyed in terms of their approach to implementing BC with SDN.

TABLE 3. Approaches to implementing BC with SDN.

Approach	Proposals
Integrated	[27], [29]–[32], [34], [35], [42], [45]–[48], [52], [55], [56], [59], [67], [68]
Collaborative/ Cooperative	[37], [38], [40], [41], [50], [51], [53], [54], [58], [60]–[66]
Overlay	[33], [36], [39], [43], [44], [49], [69]

B. PROS AND CONS OF BC-SDIoT

The combination of BC and SDN in addressing IoT issues is compelling. In this context, BC and SDN serve as complementary technologies that mitigate the known disadvantages of IoT devices [5]. IoT devices' hardware simplicity often renders them incapable of significant computation, such that they may be collectively incapable of executing complex security protocols, including implementing BC. Their massive numbers also make solutions difficult to scale due to the requirement that any BC-enabled SDN solution must implement an effective underlying infrastructure to handle a large and dynamically varying number of IoT devices.

The advantage of the combination of BC and SDN is that we can create scalable and flexibly managed infrastructures capable of interacting with large numbers of IoT devices. SDN manages the network while BC mitigates SDN's single-point-of-failure nature, and both technologies may be combined to facilitate the implementation of effective security services within the network.

The disadvantages of combining BC and SDN with IoT devices typically lie in the underlying challenges faced by IoT devices themselves. Since IoT devices may be susceptible to security attacks, BC-enabled SDN implementations face challenges in isolating these types of faults. Indeed, some of the research efforts attempt this by presenting an architecture in which small sub-nets of IoT devices are organized into clusters that may employ localized fog/edge computing providing access to the network. These localized clusters may be susceptible to security attacks because the IoT devices may not be capable of self-protection. However, the organization into clusters protected by BC and SDN technologies can help to localize any damage and provide early detection and fast response to attacks.

Still, this represents one significant open issue or disadvantage to this approach: the IoT devices themselves are naturally insecure, and it remains a challenge to completely overcome this problem using BC and SDN technologies. Yet, the security posture improvement of such an approach is still significant.

IV. RELATED SURVEYS

There have been several surveys previously published addressing various combinations of networking technologies, including BC, SDN, and IoT. Table 4 gives an overview of these studies, chronologically introduced below. To the best of our knowledge, there are currently no surveys in the

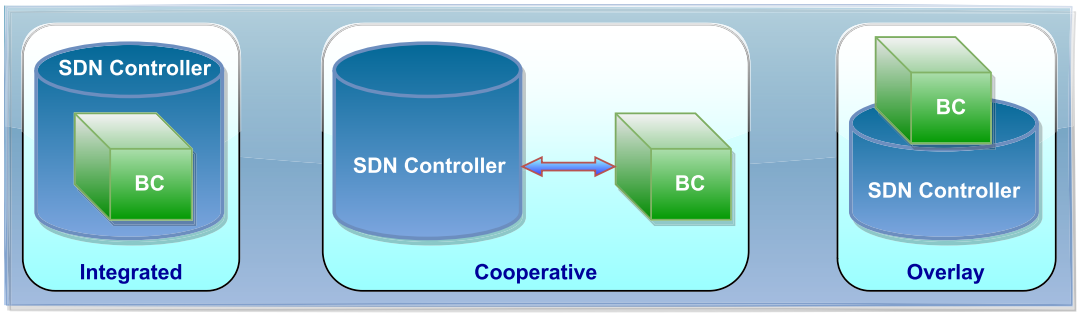


FIGURE 7. BC-SDN approaches.

literature that specifically feature the integration of all three network architectures, that is, the integration of IoT with BC and SDN, in the depth covered within this paper.

The study in [70] reviews earlier studies that combined SDN and BC technology to create strong cyber-security solutions for shielding the SDN architecture from threats. Despite significant advancements in research, there is still a need for intrusion detection and threat mitigation that can safeguard the control and data planes as well as the communication channel. In order to secure SDN security and provide a chance for a more scalable and effective SDN architecture, the paper also provides a strategic vision for adopting BC technology and leveraging its advantages.

The authors in [71] examine current security problems and their potential countermeasures for blockchain-based SDN. Specifically, this work introduces the most current research efforts related to the general structure of BC-based SDN. The authors also discuss several security vulnerabilities (e.g., scanning, spoofing attack, hijacking attack, etc.) and the solution to these weaknesses through techniques, such as traffic and flow control, policy enforcement, and Denial-of-Service (DoS) defense.

In order to propose an SDN data chain based on BC that realizes the consistency of data records and breaks manufacturer isolation, improves network fault resistance, and achieves unified scheduling of business capabilities, the authors of [72] organize the current development status of BC-SDN in terms of consensus algorithms, encryption guarantees, data security, and log transparency.

To examine the possible advantages of BC technology when applied to future Data-Driven Networks (DDNs), the authors in [73] analyze the related pioneering research works in the survey and their uses in computer networks. When considering the distinctive features of BC technology, several research problems (e.g., privacy, security, authentication) are also recognized for Blockchain-empowered Data-driven Networks (BDNs). Their research paves the way for the creation and implementation of future BDNs by providing a deeper knowledge of how BCs might be included in future DDNs to enhance the functionality of data-driven apps and network management.

The research in [74] provides an overview of blockchain SDN in healthcare in terms of using the BC benefits for network traffic prioritization, lowering occurrences of failure, changes in track configuration, suitability for mergers and acquisitions, data sharing, personal identity, maintenance of personal health records, insurance claim, and auditing.

The authors of [75] give the first in-depth analysis of BC-based Border Gateway Protocol (BGP) inter-domain routing security solutions. According to the type of BC being used, the research systematically classifies and identifies outstanding problems that need to be solved and offers fundamental knowledge to researchers interested in this field. This survey also compares and analyzes their limitations, scalability, level of protection against BGP assaults, performance metrics, and capabilities.

In [76], the authors analyze current BC technologies used with SDN from both security-aware and security-agnostic perspectives. The background information on BC technology and its current consensus methods were presented, and the study examined various current polls along with their flaws and restrictions.

The work in [77] describes the design principles of the BC paradigm, gives an overview of common security concerns with SDN when connected to IoT clouds, and argues for the benefits of using BC as a significant security factor for solutions involving SDN and IoT. Furthermore, the research presented in this position paper was intended to serve as the foundation for a more thorough investigation into the potential applications of BC.

Similarly, the survey presented in [78] presents an overview of the literature background on BC and SDN, with a broad presentation of BC-SDN integration discussing the benefits and limitations of BC-SDN approaches. In the survey, the authors address the key features of the BC-SDN ecosystem, the main security and privacy weaknesses of BC-SDN, and the integration of BC-SDN to new smart system applications (e.g., healthcare system, supply chain management, e-voting, etc.).

The study in [79] presents a good overview of intrusion detection approaches (e.g., anomaly detection, misuse detection, etc.) in SDN-based IoT networks while applying Machine Learning (ML) and Deep Learning (DL) techniques.

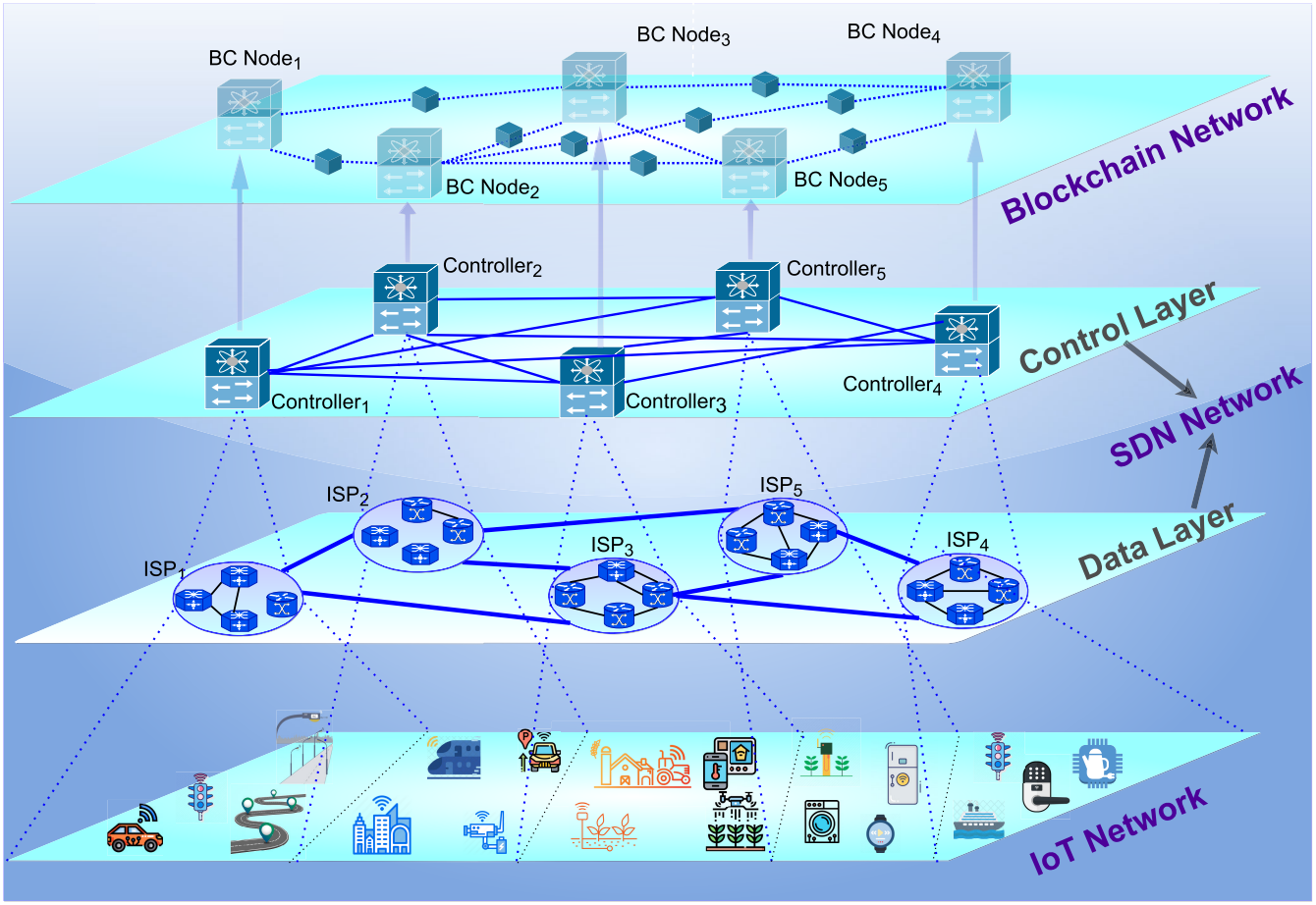


FIGURE 8. General structure for the integration of BC and SDN in IoT (BC-SDIoT).

Although it addresses the potential integration of BC with SDN and IoT, it does not comprehensively survey approaches in which BC has been integrated.

The authors of [80] and [81] analyze the resource constraints, centralization of the identification and authorization, and privacy issues to track and monitor users' personal data throughout IoT applications and devices by integrating BC technology into SDN infrastructure. In the survey, the authors explore the convergence of blockchain and IoT for security-based weaknesses due to the lack of using traditional security mechanisms with limited resources and energy capacities of IoT devices. The fundamental cryptographic methods used in BC's current implementations are thoroughly discussed. Additionally, the authors recommend using lightweight cryptography to improve the security features of IoT devices with limited resource availability.

The authors in [82] review blockchain, SDN, and Network Function Virtualization (NFV) for smart-home security. The study proposes a smart-home security architecture and discusses smart-home features and security challenges. Furthermore, the paper describes blockchain, SDN, and NFV and how they improve smart-home security. SDN gives home nodes a programmable controller to manage and regulate the home network, while NFV virtualizes network equipment like firewalls and monitors to assure network availability. Blockchain enhances IoT data privacy, integrity, security, and trust in transactions between untrusted devices.

In [83], the authors elaborate on increasing requisites and the use of SDN and IoT designs for resolving these features for Industry 4.0 by trying to support the integration of artificial intelligence and blockchain, as well as analyzing the future research prospects and the usability impact of these architectures.

While all of these surveys have been comprehensive, they have not specifically addressed integration and related issues of IoT with the technologies of blockchain and SDNs, except for [83], which focuses primarily on the technical details of Industry 4.0. Our survey differentiates itself by placing a primary focus on the integration and related issues of IoT with the technologies of BC and SDN.

A very recent survey of blockchain in SDN IoT with NFV for smart applications is presented in [84]. While it provides very good coverage of the individual components of BC, SDN, IoT, and NFV, the BC-SDIoT coverage as a complete system is very limited and at a very high level. Further, their focus is smart applications. In our paper, we approach

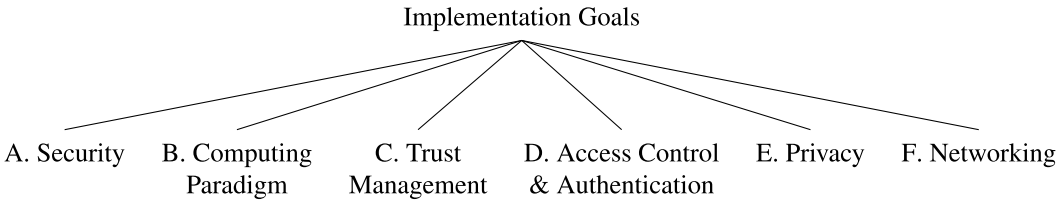


FIGURE 9. A high-level classification of proposals in BC-SDIoT from the perspective of implementation goals.

BC-SDIoT at a fundamental level with special emphasis on infrastructure, security, trust, and data management from a system research perspective. Further, in contrast to the approach in [84], we include several taxonomies of BC-SDIoT from different angles.

V. SDN AND BLOCKCHAIN EMPLOYED IN IoT (BC-SDIoT)

The general structure for integrating BC and SDN in IoT (BC-SDIoT) is depicted in Fig. 8. The structure consists of four main layers: IoT layer/network, data layer, control layer, and BC layer/network, where the data and controller layers comprise the SDN network that holds multiple Internet Service Providers (ISPs). The IoT network accommodates smart devices collecting information from the environment. While the data layer consists of OpenFlow-enabled infrastructure devices such as switches and routers, the SDN network controllers reside in the control layer. Finally, the top layer is the BC network, where network controllers build a BC network to maintain a distributed shared ledger keeping transactions representing network state or data (such as topology, devices, flows, etc.) related to either SDN or IoT networks. These controllers act as representatives for the BC-participing nodes. As noted in Section III, the BC layer may be integrated with, cooperating with, or an overlay on top of the SDN control and/or data layers.

Fig. 9 presents a high-level classification of various problem domains addressed in the literature for the integrated SDN-BC approaches, discussed in the following subsections, into six main categories based on the published literature: Security, Computing Paradigm, Trust Management, Access Control and Authentication, Privacy, and Networking. The details for each are given in the following subsections.

A. SECURITY

A significant portion of the constantly evolving computing paradigm is to be provided by the anyplace, anytime, anywhere, anything IoT ecosystem. This, in turn, offers tremendous opportunities for new services that may improve aspects of our personal lives, gain efficiency, reduce errors, and increase production capacity in business. Nevertheless, there is a consensus on the subpar cyber-security techniques in the IoT ecosystem to safeguard ourselves against many adversaries [5], [85]. The combination of SDN with BC provides a viable and promising solution to these cyber-security challenges in IoT.

Numerous approaches, as shown in Fig. 10, have examined attack detection, mitigation, and prevention, as well as cloud security. A number of studies are classified as general security approaches and may either state less specificity or include multiple techniques in our taxonomy. The taxonomy is also outlined in Table 5, which provides a brief statement of each work's objective(s), along with solution techniques.

1) ATTACK DETECTION AND MITIGATION

In general, attack detection and mitigation can be considered complementary efforts that may be addressed in combination. The works in this area focus on approaches to one or both of these. Additionally, many studies focus on Distributed Denial of Service (DDoS) attacks, including TCMP/SYN flooding, TCP and/or UDP flooding, and ICMP flooding. The differences lie in their respective approaches to detection and mitigation.

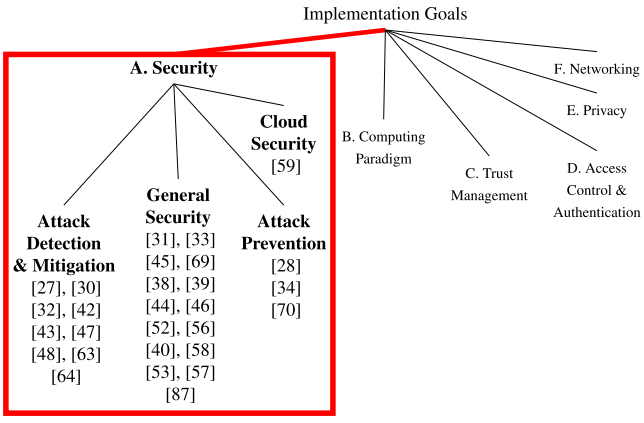


FIGURE 10. Classification of proposals in BC-SDIoT from the perspective of implementation goals for the security category.

Several works employ deep learning approaches to train the network to discern between valid and attack data. [26] proposes a distributed attack detection system using an Ethereum BC for IoT networks. The method focuses on dynamic traffic flow control and addresses TCP and ICMP flooding and DDoS attacks. BC is employed to prevent attacker injection of undesirable data at fog and edge networks. The BC uses a deep learning approach to train the SDN by classifying and identifying traffic types and mitigating the attacks. Based on early detection and classification, the mitigation strategy is to prevent further malicious data from entering the system, reducing the chances of attack.

TABLE 4. An overview of the surveys addressed the use of BC with various networking technologies.

Reference	Target Domain	Summary
[70]	Security	Focus on analysis of the current implementation of Blockchain technology in SDN for security purposes by asking questions and address the limitations of proposed solutions.
[71]	Security	Discussion on potential security issues and relevant solutions in BC-enabled SDN implementations.
[72]	Data management	Discussion on current development status and existing problems of software-defined data-chain network based on BC.
[73]	Data-Driven Networks	Survey on the challenges and potential solutions in BC-empowered future Data-Driven Networks (DDNs) and traditional computer networks.
[74]	Security in healthcare	An overview of BC and SDN in healthcare to provide security, privacy, and integrity to the health care data.
[75]	Secure BGP-based inter-domain routing	Discussion on how BC can provide an alternative in order to prevent the false origin of IP prefixes or hijacking AS paths.
[76]	Security/Non-security in IoT networks	Summary of approaches applying BC and SDN for security and non-security issues as well as challenges existing challenges in the BC and SDN based IoT networks.
[77]	Security in IoT Clouds	An overview of common security issues of SDN-based IoT clouds.
[78]	Security and Privacy	Survey on security and privacy issues of BC and SDN integration considering applications and challenges in real implementations.
[79]	Security in Intrusion Detection Systems	A brief discussion on SDN and BC enhanced IoT to enhance security in Intrusion Detection Systems.
[80], [81]	Security	Focus on how BC can be converged with (SDN-based) IoT system to improve security aspects.
[82]	Smart-Home Security	Discussion of smart-home vulnerabilities,
[83]	Industry 4.0	High-level description of SDN, IoT, Industry 4.0, Blockchain and AI
[84]	Smart Applications	Comprehensive coverage of BC-SDN with NFV supporting smart applications

TABLE 5. Classification of studies regarding objective and solutions to security approaches.

Problem Domain	Source	Objective	Solution
Attack Detection & Mitigation	[26]	Early and efficient DDoS detection	SDN dynamic rule update based on anomaly detection using BC with fog and edge
	[29]	Early and efficient DDoS detection	BC with SDN and fog to eliminate single POF and quickly detect attacks
	[31]	Defense against DDoS attack	SDN controllers mitigate attacks; smart contracts to automate
	[41]	Efficiency, Improved identification rate	BC integrated with SDN, edge-cloud, and new detection algorithm
	[42]	Evidence integrity for forensics	BC logs events in SDN IoT to detect/predict bad data
	[46]	Prevent internal hosts from becoming bots	BC with security modules to identify compromised hosts
	[47]	Secure fog computing	BC-based distributed cloud arch. with SDN
	[62]	Increasing attack surface	BC implements decentralized DDoS collaboration
	[63]	Increasing attack surface	BC implements decentralized DDoS collaboration
General Security	[30]	Prevent resource allocation double spending	BC with distributed consensus
	[32]	Security; scalability; efficiency	BC implemented in SDN controllers to maintain flow rules
	[34]	Security of IoT devices with low power	Efficient authentication with public and private BC clusters to optimize energy consumption
	[37]	Avoid SDN single point of failure	BC-based distributed control
	[38]	Avoiding malicious SDN flow rules	BC-aided flow insertion and verification
	[39]	Reduced energy consumption in secure architecture	Network Function Virtualization with new cluster head selection algorithm within an energy-aware architecture
	[43]	Security; energy efficiency; network management in smart buildings	Fast and energy-efficient cluster-head selection; load sharing across SDN devices
	[44]	Security; energy efficiency; resource management	Fast and energy-efficient cluster-head selection; and BC maintenance of SDN flow rules to ensure consistency
	[45]	Security of IoT devices with low power	SDN groups IoT devices into separate BCs based on capabilities/proximity
	[46]	Prevent internal hosts from becoming bots	BC with security modules to identify compromised hosts
	[51]	Maintaining trust between SDN control and data planes	Flow verification using edge-computing based BC as a Service (BaaS)
	[55]	Network measurement	BC added to SDN-based IoT network measurement framework
	[56]	collective SDN controller security	BC implemented in distributed SDN network
	[57]	Security and reduced power consumption	BC implemented in distributed SDN network
	[68]	Security of fog-based SDN nodes	BC for system security
	[86]	Distributed secure architecture	Distributed SDN controller with IDS
Attack Prevention	[27]	Prevent routing black hole attacks	BC-based routing information dissemination
	[33]	Prevent malicious traffic broadcasting	BC consensus algorithms (PoW, PoS)
	[69]	Sec & Privacy of Crowdsourced SDN-IoV	BC exploiting Deep Reinforcement Learning
Cloud Security	[58]	Cloud storage security	BC inside cloud storage

The approach in [29] uses another deep learning approach, which is specifically used to detect the attacks themselves. It employs a distributed SDN architecture that removes concerns over a single point of failure in a centralized SDN controller while simultaneously implementing a distributed BC that enables sharing security models among fog nodes. This sharing improves on other approaches that could not develop accurate attack models due to fog nodes being associated with a limited number of IoT devices. The sharing of models allows the fog nodes to expand their data sets significantly to improve attack detection accuracy. The authors identified areas for improvement in other approaches,

including single-point-of-failure issues with centralized SDN controllers and the difficulty of edge and fog nodes in developing accurate models due to the lack of available data. This approach implements a distributed SDN architecture to mitigate the single point of failure problem, along with an architecture in which fog nodes share their models among themselves to gain more data and improve the accuracy of their models.

The study in [41] employed a different approach that assumes trusted IoT nodes are known in advance, with authorized IoT devices placed in groupings according to geography. The attack detection mechanism places responsibility on gateway nodes at the edge-cloud layer, which implements SDN and BC to improve security and performance. The edge-cloud servers aggregate and authorize transmission of IoT data and serve as management front-ends to the IoT devices. The approach improved throughput and packet data rate while reducing packet jitter and energy consumption in the network.

Another approach is to employ BC to store network information allowing the SDN to discern valid traffic from an attacker. In [46], the authors proposed a mechanism specifically focusing on the detection of botnets, with detection occurring in the SDN controllers themselves. The mechanism employs BC with SDN to automatically detect changes to the system data plan, topological features, and flow status. In this approach, the BC is extended to use a colored coins approach, in which bitcoins are marked to contain specific assets. The assets are the markings of IoT nodes meeting minimum security requirements to provide an additional level of security by allowing SDN controllers to distinguish authorized vs. unauthorized traffic more efficiently.

Reference [42] employs a forensic detection approach that uses automatic features of SDN in combination with additional new features. The data plane of the SDN will automatically discard packets not obeying flow rules and automatically migrate packets in cases of overloaded switches. The control plane is employed to validate devices using a linear homomorphic signature algorithm, further classifying the devices using a neuro multi-fuzzy network. One stated advantage of their approach lies in the authentication using LHS. Instead of using unique identities that might be predicted or forged by attackers, the LHS uses the device identity in combination with a unique elliptic curve point chosen by each device, which helps to prevent identity forgeries. Forensic activities employ packet analysis to detect malicious activities by examining logs of the classified packets. The authors of this study compare its performance with that of [47], although the work in [47] is not explicitly focused on forensics. Performance improvements were found in delay, response time, throughput, and processing time.

DDoS mitigation is addressed in [62] and [63]. This approach employs a decentralized BC using smart contracts. The BC is used to store network flow rules to track suspicious traffic, while the smart contracts are used to store information on suspicious nodes, so that authorized participants may receive access to the list of nodes to be blocked. Accordingly, smart contracts enable peers being attacked to automatically propagate lists of suspicious hosts while taking action in a collaborative fashion.

2) ATTACK PREVENTION

The approach described in [46] (also presented above as a detection scheme) combines attack detection with a level of mitigation to effect attack prevention. The work considers attacks on the network of SDN controllers, wherein their distributed botnet detection scheme addresses problems with large numbers of IoT devices using a network of distributed SDN controllers that implement a distributed BC. Each controller participates in the implementation of policy, control, and log modules; controllers exchange authenticated flow rules that are verified using the BC. The colored coins approach is used to label IoT devices and determine which may be in botnets so that traffic is readily filtered and attacks are prevented.

By addressing features of an Intelligent Transportation System (ITS), the authors in [33] address attack prevention by ensuring message-passing systems that are immutable, credible, and authentic while simultaneously preserving user privacy. They based the study on the premise that Vehicular ad hoc networks (VANETs) are typically composed of large numbers of vehicles that automatically do not trust each other. The work examined the use of vehicle trust scores to prevent the existence of counterfeit or forged information. It features a blockchain-based security framework that supports vehicular IoT services, including real-time cloud-based video reports and trust management in vehicular messages. Vehicles uploading information to the VANET have a trust score assigned to their messages by nearby vehicles already authenticated in the network. Privacy is preserved by storing vehicle authentication information separately from user identities. The SDN data plane consists of all vehicles in the VANET, while the control plane implements policies, authentication, and traffic management functions. BC is implemented in RoadSide Units (RSUs) to store trusted traffic information.

Another study addressing vehicular networks places its focus on SDN-IoV networks. To improve data collection and processing, an SDN-based architecture with multi-access edge computing built on top of a spatial crowd-sourcing [87] is introduced in [69]. The study addresses effective means to deal with large numbers of computational tasks in SDN-IoV networks. Due to network constraints, the vehicles rely on spatial crowd-sourcing to request and receive various tasks in the network. The problem addressed is ensuring the privacy of the vehicles' users while simultaneously acknowledging that they need to be fully trusted. Multiple BCs are used to prevent a single point of failure and for privacy preservation against collusion and Sybil attacks. A novelty is that a deep reinforcement learning algorithm also allocates ITS tasks

to select the consensus algorithm, block size, and block generation rules.

In a secure routing architecture, [27] uses smart contracts storing abstract topologies along with SDN controllers' reputations to ensure secure routing and prevent black-hole attacks. The SDN is used to implement a more flexible and agile IoT network. In this architecture, local topologies are abstracted to preserve privacy within local domains. These abstract topologies, along with the reputation scores of the SDN controllers, are shared and recorded in the BC, creating a secure global view of the network topology. The authors found the architecture effective at building global trust between multiple controllers and protecting routing reliability among multiple domains.

References [38] and [51] address the problems of flow conformance and tampering with messages between controller and switch. This is accomplished through BC as a Service (BaaS), which is used to verify inserted flows. The authors also noted that using an external BaaS obscures knowledge of agents responsible for flow conformance testing. They also introduce a strategy that prevents these agents from acting arbitrarily. The strategy is based on a mathematical model of a fair reward scheme in game theory. Their results introduce a measurement of *social welfare*, a measure of profits of verifier and verification initiator. The study demonstrated that the mechanism creates a balance among blockchain agents by maximizing social welfare among all participants.

Gao et al. [37] examine data security and privacy in a pervasive edge computing (PEC) environment. Their specific goal was to develop a secure data-sharing model. Their approach combines identity-based proxy re-encryption (IBPRE) with a consortium blockchain implemented in an SDN-enabled PEC environment. BC is used to store crypto keys, and users can make updates using smart contracts. The system is also employed to authorize IIoT devices to provide reliable and credible connectivity to the PEC environment.

3) GENERAL SECURITY

The works classified as *general security* included a variety of approaches that were not always as easily classified. One aspect includes attack defense, similar to mitigation strategies while providing additional protection. We start with several works that propose general security frameworks, each of which could be used to implement several specific security initiatives.

Reference [31] proposes a security framework that employs a hierarchical organization of SDN controllers to implement multiple BCs to enforce security. A global BC is employed by decentralized SDN controllers, storing source IP addresses that are allowed or blocked. Network segments attached to the primary network employ private BCs to store transactions, and they employ smart contracts for access control. The SDN controllers in each segment respond to attacks in the specific segment, and mobile agents are employed to connect each segment BC to the global BC.

Reference [32] proposes an architecture, *DistBlockNet*, in which a BC controls flow rule tables to ensure their validity. The architecture implements a global BC among a decentralized SDN controller network, with controllers for local network segments maintaining several modules to handle security threats at different levels. The local network view modules implement access control, data protection, and threat intelligence at the management and application layers and flow control and packet analysis at the data and control layers. In performance comparisons with existing distributed SDN controllers without their architecture implemented, the DistBlockNet was shown to provide superior bandwidth for nodes in the network.

Reference [45] presents a design of architecture intended to accommodate IoT node capabilities, in which IoT nodes are clustered into BCs based on their computational capacity and proximity to an SDN switch. IoT nodes act as blocks in a BC implemented directly on an Open vSwitch. Reference [43] proposes a broad security approach employing BC and SDN to store and securely transmit information among IoT nodes in a smart building. The approach implements a distributed BC to secure smart lighting, firewalls, switches, and camera services for an intelligent building control system. A significant aspect of this study is the cluster head selection algorithm for IoT devices, which seeks to optimize communication and reduce energy consumption.

Another approach to addressing energy consumption is presented in [44], which also seeks to answer broad questions of efficient deployment of IoT in distributed networks, as well as suitable security enhancements of an SDN-enabled distributed system. Similar to the approach in [43], the authors developed a new cluster head selection algorithm to optimize communication and reduce energy consumption. The authors also proposed developing a layered hierarchical approach to developing a blockchain-enabled IoT network. The BC is employed in their approach to track and enforce consistency of flow rules within an SDN. Security is enforced when switches not following rules are blocked from participation in the network.

The main focus of the work in [30] is to present a wireless virtualization framework to enable the operation of virtual wireless network operators (VWNOs). The idea is for SDN to facilitate dynamic configuration and efficient management of network resources, employ edge computing to improve network performance and utilize BC to ensure that RF slices are not allocated to two separate communications, noted as a form of a double-spending attack.

In [56], the primary focus is on ensuring cooperative management among controllers from different operators while simultaneously ensuring the security of the SDN controllers. It employs a novel approach to overcome the low efficiency of BC through the use of sharding, as illustrated (for example) in [88].

The approach in [57] is to connect the network of SDN controllers using a public BC while employing them as cluster heads managing IoT devices with private

BC implementations. The authors developed an associated routing algorithm that performs well in terms of throughput, delay, and power consumption.

A high-level distributed SDN controller architecture enhanced with an IDS is proposed in [86] where implementation in the open-source OpenDaylight controller.

Network management relies on accurate network traffic measurement and estimation, yet it is elusive and challenging. The simplified network management of the SDN paradigm, combined with the authenticity, credibility, transparency, and reliability provisioning of BC, comprise the foundation of the approach proposed in [55] for IoT networks. Fine-granularity traffic estimation is formulated as an optimization problem based on the coarse-granularity counterpart and an ant colony, and a solution based on heuristics is provided since the original problem is NP-Hard.

4) CLOUD SECURITY

Efficient cloud storage security is addressed by [58], which focuses on privacy-related issues. The architecture, *Block-SDotCloud*, implements a BC at the cloud layer to enhance security and privacy in a cloud, also facilitating load balancing among SDN controllers.

B. COMPUTING PARADIGM

The computing paradigm has played a significant role in several works, as categorized in Fig. 11 and outlined in Table 6. The efforts are focused on edge and fog computing, and notably, some authors equate fog computing with edge computing [89], [90], while others consider fog to be a version of the edge more suitable for IoT networks [68]. Nevertheless, others classify various cloud-based technologies according to use cases [91]. Extending cloud services to the edge or fog means placing computing infrastructure at the network's edge to make it physically closer to the IoT nodes. This often is pursued to reduce latency and potentially provide early processing of data being offloaded to the cloud and ensure high availability, real-time data delivery, scalability, and security.

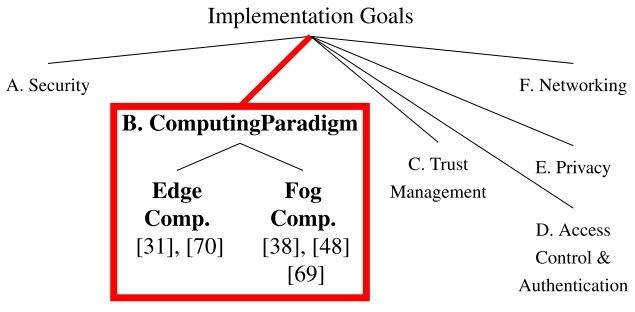


FIGURE 11. Classification of proposals in BC-SDIoT from the perspective of implementation goals for computing paradigm category.

In recognizing the drawbacks of cognitive radio network approaches, [30] proposed an approach in cellular 5G/6G that fuses SDN, edge computing, and BC for wireless network virtualization. Virtual wireless network operators share RF slices with wireless users, and the BC protects users from allocating the same RF slice to multiple virtual networks while increasing trust.

A network architecture combining SDN, BC, and fog computing is provided in [47], where fog nodes localize computing to the extent possible to reduce processing delay and improve other performance issues, such as availability, scalability, and security. The study exploits the concept of edge computing by using fog nodes that localize computing to reduce the delay associated with processing in a centralized cloud computing paradigm. A distributed peer-to-peer cloud storage solution for IoT devices with the help of base stations, likely 5G or 6G, facilitates fog layer nodes with BC-enabled SDN controllers, which are interconnected with the other fog nodes employing a centralized BC-based cloud layer. A similar approach in [68] proposes a BC-enabled SDN network to handle IoT devices by adding a fog layer between sensing and cloud-based computing. SDN provides flexibility and management (aka *orchestration*), the BC serves as a general structural component for security, and the fog layer facilitates a data offloading algorithm from the cloud to the fog to reduce end-to-end latency for computational tasks. [37] cites pervasive edge computing (PEC) as an emerging paradigm for IIoT, and their approach addresses PEC issues with data security and privacy by employing BC and proxy re-encryption to enable IIoT nodes to share data securely. Smart contracts are also employed for searching and updating BC records.

C. TRUST MANAGEMENT

We focus on the trust management category in this section, as categorized in Fig. 12 and outlined in Table 7.

One form of trust management is designed to ensure cooperation, through consensus, among BC participants. Studies reported in [53], [61], and [60] consider the problem of achieving consensus among multiple controllers in a software-defined Industrial IoT. A permissioned BC maintains a network-wide view among multiple SDN controllers. A trust feature model is coupled with other approaches to represent node states in a deep Q-learning approach to reach a consensus.

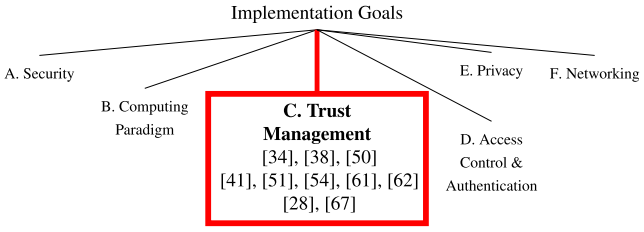


FIGURE 12. Classification of proposals in BC-SDIoT from the perspective of implementation goals for the trust management category.

A different approach uses a scoring mechanism for nodes participating in the network. In recognizing that most

TABLE 6. Classification of studies regarding objectives and solutions to computing paradigms.

Problem Domain	Source	Objective	Solution
Edge Computing	[30]	Near real-time computing to IoT devices	Edge computing facilitated by SDN controllers
	[69]	Delay-sensitive processing of IoV data	Multi-access Edge computing in SDN-IoV
Fog Computing	[37]	Avoid frequent handovers to improve performance	Fog computing under SDN
	[47]	Low-delay processing of IoT data	On-demand distributed cloud over SDN
	[68]	End-to-end latency for IoT applications	SDN-controlled fog computing layer

TABLE 7. Classification of studies regarding objectives and solutions related to trust management approaches.

Problem Domain	Source	Objective	Solution
Trust Management	[27]	Ensure routing reliability among SDN controllers	Reputation-based trust management
	[33]	Prevent malicious or inaccurate information	BC-based trust management
	[37]	Trustworthy peer information	BC to establish message trustworthiness
	[40]	Device authenticity	BC-based trust list to verify IoT services and devices
	[49]	Privacy preserving secure patient records	SDN Trust Module w/ trust value calculations
	[50]	Scalable storage and management of IoT public keys; trust	BC stores public keys with SDN providing efficient routing
	[53]	Consensus in software-defined Industrial IoT	Dueling deep Q-Learning approach
	[60]	Consensus in software-defined vehicular networks	Dueling deep Q-Learning approach
	[61]	Consensus in software-defined Industrial IoT	Dueling deep Q-Learning approach
	[66]	Risk management for home IoT devices	SDN groups devices into isolated slices with BC to disseminate trust reports

TABLE 8. Classification of studies regarding objective and solutions to access control and authentication approaches.

Problem Domain	Source	Objective	Solution
Access Control	[34]	Secure IoT device access control	Public and private blockchains
	[49]	Privacy preserving secure patient records	SDN authentication & authorization module
	[54]	Address vulnerabilities between controller and application SDN layers; address single PoF issues	Certificate-based access control incorporating attribute-based encryption implemented in distributed private BC
	[59]	Ensuring consistent access control policies for servers	BC employed to load balance and implement access policies
	[64]	Authentication of service requests	BC employed to validate service requests for smart IIoT data services
Authentication	[33]	5G-VANET vehicle authentication with privacy	Separate user and vehicle authentication
	[36]	Authentication of relay nodes, and optimized routing	Lightweight Registration Authentication with BC storing IoT credentials and malicious node list; and genetic algorithm-based SDN routing
	[40]	Authenticating IoT devices and preventing unauthorized traffic	BC-based trust luist to verify IoT services and devices
	[42]	Verifying sources in SDN IoT	Linear Homomorphic Sign. for authentication
	[48]	SDN controller's single point of failure	BC's decentralized operation
	[50]	Scalable storage and management of IoT public keys with authentication	BC facilitates authentication by storing public keys of IoT devices
	[65]	Efficient authentication handover in 5G	BC and SDN employed to eliminate unnecessary re-authentication

vehicle occupants do not trust each other due to anonymity, the authors in [33] developed a trust management system combined with BC in a vehicular IoT environment using a radio access network over a 5G infrastructure. Cars upload real-time videos and current traffic conditions, which are scored for accuracy and are used as a trust computation. The BC enhances security and preserves privacy by separating user identity from operators of vehicles.

The work in [50] presents an architecture in which SDN is used to route network traffic, and BC is used to store keys and the trust history of IoT devices. IoT devices register key pairs, communicate securely, and provide feedback to the BC to record whether communications are trustworthy. The approach outlined in [37] is to employ several critical servers as BC participants, such as a policy management server that employs smart contracts to establish penalties for vehicles providing false information, with trust being administered through the BC.

Home networks of IoT devices suffer from the lack of acceptable security measures and often present an easy target for adversaries [5]. SDN-based home networking in [66] is proposed to group connected IoT devices into simplified risk management levels from ISO/IEC 3100:2018 where trust scores of device classes are computed from the crowd-sourced data. BC serves as the immutable and trustable platform to store trust scores.

D. ACCESS CONTROL AND AUTHENTICATION

Fig. 13, along with Table 8, provide the focus of this section. Reference [59] employs a permissioned BC-based SDN, in which controllers maintain access policy/security information in the BC and is found to improve performance in the face of spoofing and DDoS. The approach employs digital signatures as authorization tokens controlling access to specific resources. [34] employs a combination of public and private BCs to provide P2P communication and secure access control for IoT devices.

In [48], the network management characteristics of SDN combine with a public BC among SDN nodes in multiple domains and a private BC that eliminates PoW among IoT devices and SDN controllers, providing enhanced generic security and reduced energy consumption. Reference [54] presented a robust access control scheme using a private BC that alleviates a variety of well-known security threats. The mechanism also facilitates centralized administration

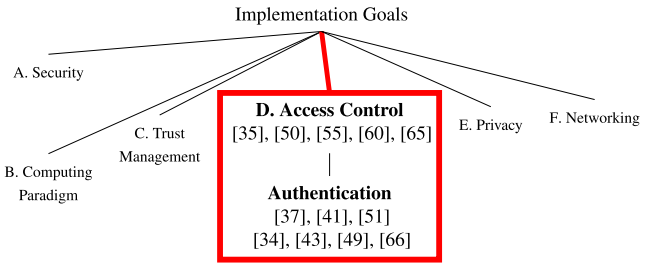


FIGURE 13. Classification of proposals in BC-SDIoT from the perspective of implementation goals for the access control and authentication category.

and performs well compared to comparable schemes. Reference [49] employs an access module in a broader effort toward a trust management system for patient healthcare information. The access control module grants access to applications based on a trust level established by a trust module. The forensics architecture in [42] also employs a linear homomorphic signature algorithm in its BC implementation for user authentication.

Reference [36] proposed the use of a lightweight BC-based authentication mechanism in which IoT device credentials are stored in a BC to achieve lightweight authentication. *Trust List* was proposed in [40], representing a distribution of trust among IoT-related network devices and providing autonomous enforcement of IoT traffic at the network's edge by integrating SDN and BC.

Reference [64] presented an architecture employing a BC above the SDN control layer, in which the BC receives requests through the SDN for services related to IIoT data. The BC is employed to validate service requests from the database stored in the cloud.

Reference [65] presented an architecture used to improve authentication efficiency in 5G networks that may include IoT devices. The architecture employs a BC to store registration and identification information for mobile units that may move among different cells. Registration information is transmitted from the BC to the SDN controller of the relevant cell, which shares this information with access points in its current cell, as well as with controllers of adjacent cells. This eliminates the need for re-authentication when handover occurs while the mobile unit is moving among heterogeneous cells.

E. PRIVACY

In Fig. 14 and Table 9, we highlight the privacy category for our following discussions.

A healthcare monitoring system, with sensors forming a Body Area Network (BAN) at the outermost edge connected over a 5G/6G access technology, is proposed in [49]. It includes architectural support from SDN for modular coordination based on a trust value as a function of reputation, privacy, operational, and information risk. A permissioned BC is overlaid on top to protect patient information privacy.

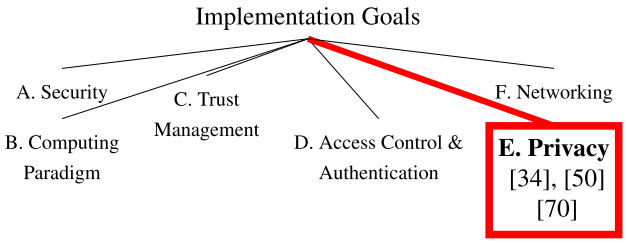


FIGURE 14. Classification of proposals in BC-SDIoT from the perspective of implementation goals for privacy.

Reference [33] developed a traffic information collection system, which includes uploading encrypted videos. The desire was to preserve users' willingness to participate under the conditions that videos could be used for evidence. Hence, their approach uses a department of motor vehicles (DMV) and a trusted authority to ensure that anonymity remains among vehicles in the system. BC is used to store trust values about participating vehicles.

F. NETWORKING

In the content area of networking, categorized in Fig. 15 and outlined in Table 10, we consider more classical networking tasks as the main goals, addressed as follows:

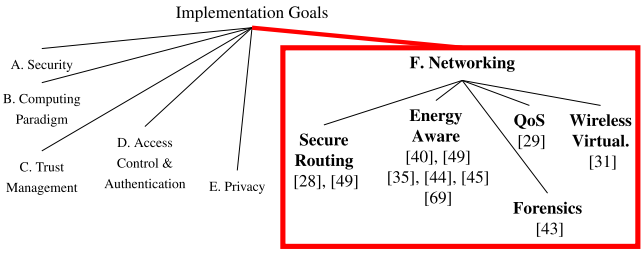


FIGURE 15. Classification of proposals in BC-SDIoT from the perspective of implementation goals for the category of networking topics.

1) SECURE ROUTING

The agility and flexibility of SDN-enabled networks provide a viable solution for the IoT ecosystem with a large number of devices organized topologically into multiple domains. However, a malicious takeover of one of the domains may easily deceive others by disseminating false routing information to attract and discard traffic, known as a *black-hole attack*. This is addressed in [27] through a multi-domain secure routing infrastructure that employs BC enhanced with a local and global reputation as a metric.

2) ENERGY AWARENESS

A variety of approaches maintain energy-awareness to minimize power consumption. The work in [34] employs public and private BCs for peer-to-peer communication among IoT nodes and SDN controllers. BCs eliminate PoW and use efficient authentication methods executing on resource-constrained IoT devices to minimize energy

TABLE 9. Classification of studies regarding objective and solutions to privacy approaches.

Problem Domain	Source	Objective	Solution
Privacy	[33]	Prevent malicious traffic broadcasting	BC consensus algorithms (PoW, PoS)
	[49]	Privacy preserving secure patient records	SDN Trust Module w/trust value calculations
	[69]	Data privacy in IoVs	BC empowered spatial crowdsourcing with DRL

TABLE 10. Classification of studies regarding objectives and solutions to networking.

Problem Domain	Source	Objective	Solution
Secure Routing	[27]	Global trust among cross-domain SDN controllers	BC-based routing information dissemination
	[48]	Improved communication security and optimized energy consumption	Private cluster BC with public BC for inter-domain routing
Energy Aware	[34]	Reduce IoT device energy consumption	Efficient cluster structure with private BCs to optimize energy consumption
	[39]	Preserving IoT device energy	Energy-aware CHS algorithm
	[43]	Preserving IoT device energy	Energy-aware CHS algorithm
	[44]	Preserving IoT device energy	Energy-aware CHS algorithm
	[48]	Preserving IoT device energy	Energy-aware private/public BCs and energy-sensitive SDN cluster structure
	[68]	Preserving IoT device energy	SDN with distributed fog computing architecture
Forensics	[42]	Detection of criminal activities	SDN integrated with BC and IoT
QoS Provisioning	[28]	Provide QoS guarantees to end user	BC stores transactions among service requestors and providers; Game theory used to negotiate service contracts that are stored in the BC
Wireless Virtual.	[30]	Efficiency and security in wireless virtualization	SDN for management, BC for security

usage. Reference [43] employs a new cluster head selection algorithm, where a cluster head interacts with IoT-enabled SDN gateways.

An energy-optimizing approach is also used in [39] for cluster head selection and communication. The paper presents a layered architecture of a smart city/cloud connected to a network of IoT devices. The architecture includes a perception layer consisting of IoT devices, an edge layer that provides processing of perception layer data, and a cloud layer for storage. The BC is employed to store IoT device addresses securely. Energy savings are realized in the perception layer through efficient cluster head selection and the employment of network function virtualization [92] for IoT communication.

A similar approach in [44] adds BC-enabled flow rules to track and maintain consistency within the controller clusters. The approach in [68] is to use SDN with distributed fog computing to bring cloud computing capabilities close to IoT nodes and thus improve energy efficiency.

3) QoS

QoS provisioning is briefly addressed in [28]. The architecture uses BC with smart contracts implemented on SDN switches interacting with IoT sensor nodes. QoS rules and services agreements are implemented by smart contracts.

4) FORENSICS

A single work was identified that specifically addresses forensics [42]. The approach has packets being classified and logged on the SDN controllers for subsequent examination by forensic investigators. Security of the information is maintained through the implementation of a BC on the controllers.

5) WIRELESS VIRTUALIZATION

As mentioned previously, the work in [30] addressed the drawbacks of cognitive radio approaches in wireless network virtualization. In this case, BC protects network users from double-spending by double-allocation of RF slices.

VI. OPEN CHALLENGES AND FUTURE DIRECTIONS

This literature review revealed a number of categories presenting open challenges and avenues for future work.

IoT challenges have been identified as security, privacy, interoperability, and performance/scalability. Security issues [5] in IoT derive from the devices' simplicity overall; they tend to be constrained by limited power and are built with low-capability CPUs, relatively small memories, low network bandwidth, etc. An IoT device is typically incapable of executing complex security protocols due to these constraints. The solutions surveyed within this paper have generally focused on implementing security within the infrastructure, using SDN and BC as the underlying technologies coupled with fog/edge computing networks or within the underlying network infrastructure itself as implemented in a cloud service.

Privacy challenges also derive from IoT device simplicity and also exist as a result of security challenges. Simply put, if an IoT device is incapable of implementing security measures, then it is likely that the data it transmits cannot preserve confidentiality. This makes IoT devices vulnerable to *Machine In The Middle (MITM)* attacks. The interoperability challenge results from the vast number of IoT devices being built. There is a great degree of heterogeneity in IoT hardware, along with software protocols implemented for communication. Performance and scalability are affected by the fact that there are an ever-growing number of IoT devices in the IoT ecosystem; as noted earlier in this paper, as of 2022 there are nearly 43B IoT devices worldwide, with

predictions of 76B by the year 2025. It seems apparent that a goal of any system supporting IoT devices is security coupled with reasonable scalability.

Open challenges within the BC-SDIoT environment are derived from existing challenges and peculiarities introduced by this combination. The following subheadings identify particular areas of opportunity for further investigation.

A. BC-SDIoT SECURITY

A number of security challenges arise. First, maintaining IoT device authenticity in the presence of localized attacks presents a challenge. A significant question is: ''how can IoT devices be initially authenticated and maintain that authentication when their hardware simplicity renders them susceptible to being spoofed?'' A related issue is preserving data privacy while transmitting from IoT devices. It remains to be seen whether IoT data encryption mechanisms [93] will prove effective at protecting data transmitted from IoT devices. Somewhat related to this is the proxy activity that may be necessary when interacting with IoT devices. Since these devices are very simple, it would serve the community well to devise proxy mechanisms allowing local infrastructure (e.g., fog/edge computing facilities) to act on behalf of the local population of IoT devices. Effective efforts in this sense will enable the well-configured BC-SDN network to isolate segments of compromised IoT devices, as well as to more efficiently authenticate well-behaving IoT devices in localized areas. Finally, for the long-run, the recently endorsed lightweight cryptography by NIST[7] may be a promising solution strategy.

B. BC-SDIoT SCALABILITY

Other challenges are related to scalability, as well as related performance issues. Many of these surveyed works present novel and apparently effective solutions, but it is unclear whether they can be scaled to a much larger network size. The performance of BC always remains in question due to questions about its computational load. It is notable that IoT devices are typically straightforward and lacking in computational and storage capability; several works surveyed here propose solutions accommodating this, but it also remains a clear opportunity for further research, especially in consensus algorithms. Efforts at providing a scalable localized edge/fog infrastructure for connecting IoT to the cloud also remain a challenge. Another effort for scalability is that of BC scalability. Various consensus algorithms exist, and many are specifically cited as limiting factors in the performance of BC. While several of the proposals surveyed here identified great improvements in alternative consensus algorithms, this remains a fruitful area of inquiry.

Further issues related to IoT devices relate to cluster maintenance. A cluster of IoT devices may be highly dynamic, and a significant question is how to maintain the cluster in the face of this dynamism, even with effective and energy-efficient cluster-head selection algorithms.

C. BC-SDIoT WITH AI/ML

ML and Artificial Intelligence (AI) techniques have been providing viable solutions to cybersecurity vulnerabilities since the days of the spam [94], [95]. While there are studies in the literature for various combinations of these technological components, such as Artificial Intelligence of Things (AIoT) [96], AI for IoT Security [97], [98], ML/AI for IoT security [99], AI for BC [100], [101], AI for SDN [102], [103], ML and SDN for IoT security [104], and ML for SDN [105], a holistic study of ML/AI for the enhancement of BC-SDIoT (while integrating SDN and BC in the scope of IoT) is lacking in terms of performance, synergy, and security/privacy provisioning.

D. BC-SDIoT IN THE METAVERSE

IoT and BC are two of the most important technologies in the Metaverse since they provide ubiquitous computing with dependability for all Metaverse operations. In the Metaverse, Virtual Reality (VR) and Augmented Reality (AR) technologies transform actual items into digital representations using IoT framework sensory networks, mandating data transmission and process automation in intelligent IoT devices without human involvement [106]. Therefore, to protect the security and integrity of the information sent from harmful agents such as malevolent users or malicious code, this automated transmission needs a method for authentication and control. Additionally, centralized administration may come with hazards such as DoS, the ability to analyze and track user activity, restricted user control over personal information, etc. Due to its benefits, such as decentralization, privacy, transparency, auditability, and others, BC may provide intelligent and efficient solutions for these demands in the Metaverse. The ubiquity of network access and real-time huge data transfer across the physical and digital ecosystems and between sub-metaverses are made possible by networking enabler technologies such as 6G, SDN, and IoT [107].

The exponential growth of IoT devices nowadays makes it impossible for the centralized management approach to handle data efficiently from start to end. Additionally, controlling a large number of different devices is not an easy task. To fulfill the demands of IoT networks' requirement for speed and accuracy in processing, connections between devices must be highly compatible. SDN's capacity to monitor all network paths and states, modify traffic flows automatically, and notify congested links in the network and other unusual network states by a centralized controller via a standardized interface like OpenFlow may be the key to unlocking this door for the IoT-conquered Metaverse world [108]. SDN makes it possible to manage massive Metaverse networks in a flexible and scalable manner because of the separation of the

[7]NIST Lightweight Cryptography Standardization Process announced a winner (Ascon family) on February 7th, 2023 for the lightweight cryptography for IoT devices, https://csrc.nist.gov/projects/lightweight-cryptography

control and data planes. This allows virtualized computation, storage, and bandwidth resources to be dynamically allocated in response to the real-time needs of various sub-metaverses.

E. BC-SDIoT AND BIG DATA

Due to its relative simplicity, an initial impression of an IoT device is that it makes a small impact on its local (wireless) network. While this is true individually, the vast numbers of IoT devices already in place today tell a different story. Even within a localized geographic region, the large numbers and variety of IoT devices have the capability of potentially overwhelming local infrastructure with volume, velocity, and variety, i.e., the three Vs of Big Data [109].

This leads to potential opportunities in future research related to big data analytics [110], as well as the management of the data. The localized infrastructure should be capable of management of the data, as well as potentially handling some of the analytics functions also required of big data processing. Localized edge/fog computing holds potential, as identified in several works surveyed here. This type of infrastructure can be expanded to increase its capability specifically for management and analytics, not to mention IoT security. Consequently, BC with smart contracts presents a potential avenue for both management and analytics of data produced by localized clusters of IoT devices. SDN combines with BC in this sense to flexibly manage the network flows toward the cloud while simultaneously potentially reducing its volume through the pre-processing occurring at local edge/fog nodes.

F. BC-SDIoT IN 6G NETWORKS

The next generation of cellular networks presents a vast opportunity for BC-SDIoT research. The technology is characterized by potentially immense improvements in network capabilities to wireless devices; some experimental results suggest on the order of many Gbps up to Tbps data rates [111]. However, 6G is not only characterized by its data rates - it is expected to support a diverse population of devices (e.g., traditional mobile phones, as well as a variety of IoT devices) [112]. Applications are also expected to move beyond current use cases to include VR and AR, ubiquitous instant communications, multisensory Extended Reality (XR), connected robotics, autonomous systems, and even wireless brain-computer interfaces [112]. As applied within the context of the IoT, we anticipate numerous opportunities for new research involving the BC-SDIoT paradigm.

Very high volumes of data will exist in these networks due to the capabilities being established by ongoing research. Built-in infrastructure (e.g., network transponders) may include embedded support for BC and SDN so that the volume is captured ''at its source'' to prevent overwhelming the network infrastructure. Current physical limitations of next-gen millimeter waves may present opportunities in physically securing network infrastructure; because the small waves cannot penetrate physical objects (e.g., buildings), it presents an opportunity to confine signals to localized areas to help establish secure network clusters.

G. BC-SDIoT IN MOBILE EDGE COMPUTING

With the advanced IoT network, the shareable amount of data in the network is growing substantially. Processing data on a cloud server is a challenge because of the quantity of data that must be stored, as well as the high bandwidth requirements [113]. In this situation, it is essential to have a computer system to process tasks at the edge environment. By using local data processing at the edge, the latency of the whole system is effectively reduced. Furthermore, since computing is split between several nodes, each node is in charge of making decisions. When there is a node failure in the communication network, the processing assignment can still be performed by the other devices in cloud networks. Mobile Edge Computing (MEC) does the same thing by moving the processing work to the edge of the mobile network. On the other hand, computing resources at the edge may be vulnerable to break-ins by a third party. Therefore, it is crucial that MEC has extremely solid privacy and security measures to protect against any possible intrusion [114]. Even though an important goal of edge computing is to act as a bridge between IoT devices to support a requested QoS, the security of MEC must be strong enough to keep sensitive user data from being changed by an intruder. In this situation, BC can help protect data security, privacy, and anonymity by using its well-known encryption methods to be provided in healthcare, smart-city, and energy distribution systems.

H. BC-SDIoT IN FEDERATED LEARNING

Federated Learning (FL) is an algorithm for ML that lets multiple devices work together to learn a distributed model while keeping the data that was generated on each device. FL enables ML models to be equipped with decentralized data while simultaneously protecting user confidentiality by the design of the system [115]. When protecting users' personal information is a top priority, many companies turn to FL as a shared ML model. A distributed method is utilized in FL to train clients utilizing local data. In this scenario, decentralized clients or nodes are trained with the help of local data, and system parameters are discussed and shared. The creation of a global model through the use of a server requires the accumulation of system or model parameters. A device that has access to a greater number of data samples makes a greater contribution to the overall global training. A device of this kind is less likely to federate with other devices containing limited data samples if it is not provided with any form of compensation [116]. Further, ML/AI techniques can potentially augment the SDN/BC integration processes through more effective and efficient mechanisms.

By utilizing BC as an alternative to the central server, the BC network enables the exchange of local model updates of the devices in the IoT network while simultaneously

confirming and paying their associated incentives. This is done to overcome the critical difficulties brought to light. Through a technique of validating the local training outcomes, Blockchain-aware FL (BC-SDIoT-FL) can avoid having a single point of failure and expand its federation to unreliable devices in a public network. In addition, BC-SDIoT-FL allows for a greater number of devices to be federated in IoT infrastructure by offering rewards proportionate to the amounts of training samples.

I. BC-SDIoT IN OTHER NOTABLE AREAS

Some other notable areas for future work include smart contracts, interoperability, portability, and applications. Many of the works surveyed include the use of smart contracts, but it is largely an area that has (so far) received relatively little attention. Similarly, interoperability and portability present open issues and future opportunities; several versions of BC, numerous SDN implementations, and thousands of IoT device types exist. Scant attention has yet been paid to ensuring interoperability and portability across these variations, suggesting that these key technologies remain immature despite their current success in the marketplace. As far as applications are concerned, we note that while [84] presented a comprehensive catalog of smart applications, only a few papers surveyed here specifically included a focus on the BC-SDIoT ecosystem. Some papers examined home networks [66], healthcare [49], and VANET/IoV [33], [69]. We expect that there will be many other application areas that will benefit from the combined application of BC, SDN, and IoT.

The review also revealed that the overwhelming majority of approaches examined architectures in which BC was added to an existing SDN-IoT application in some fashion to benefit the IoT domain. It remains to be seen whether this approach is ideal, that is, whether similar or greater benefit may be found by adding SDN to an existing BC-IoT application.

VII. CONCLUSION

Due to the great separate potentials of SDN, BC, and IoT technologies, they have attracted significant attention in research and businesses, albeit on an individual basis. Although the combination of SDN, BC, and IoT are complementary and synergistic, much less work has been carried out that takes advantage of the joint approaches. This survey has focused on using BC and SDN technologies to establish or enhance the security and performance of the IoT ecosystem. We refer to this system as BC-enabled Software-Defined IoT (BC-SDIoT).

SDN offers a revolutionary approach to network management with visibility and centralized configuration to enable fine granularity operational control. Yet, it suffers from the classical single-point-of-failure, making it an attractive target for adversaries employing a variety of malicious exploits. BC is an excellent complement for the aforementioned SDN deficiency, with its powerful distributed ledger implemented among mutually distrusting entities. This combination of SDN-BC creates a desirable infrastructure for maintaining the exponentially growing IoT networks.

In the paper, we have elaborated on the pros and cons of BC-SDIoT from multiple perspectives. We have then provided a novel taxonomy of BC-SDIoT networks from the perspective of their implementation goals and respective research challenges regarding infrastructure, security, trust management, and data management. Since BC-SDIoT is an emerging area, naturally it has many different challenges, open issues, and potential future research directions; all of these are explained in detail in order to facilitate more discussion and trigger more studies in these areas.

REFERENCES

[1] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 27–51, 1st Quart., 2015.

[2] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[4] L. Pawczuk, R. Walker, and C. C. Tanco, "Deloitte's 2021 global blockchain survey: A new age of digital assets," Deloitte Develop., London, U.K., Tech. Rep., Aug. 2021. [Online]. Available: https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html

[5] M. Alsheikh, L. Konieczny, M. Prater, G. Smith, and S. Uludag, "The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders," *IEEE Consum. Electron. Mag.*, vol. 11, no. 3, pp. 59–68, May 2022.

[6] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 2019.

[7] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[8] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54478–54497, 2021.

[9] R. Shah, "A systematic review on blockchain in IoT," in *Proc. 4th Int. Conf. Energy, Power Environ. (ICEPE)*, Apr. 2022, pp. 1–6.

[10] P. Lin, J. Bi, S. Wolff, Y. Wang, A. Xu, Z. Chen, H. Hu, and Y. Lin, "A west-east bridge based SDN inter-domain testbed," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 190–197, Feb. 2015.

[11] K. Bakshi, "Considerations for software defined networking (SDN): Approaches and use cases," in *Proc. IEEE Aerosp. Conf.*, Mar. 2013, pp. 1–9.

[12] Y. Jarraya, T. Madi, and M. Debbabi, "A survey and a layered taxonomy of software-defined networking," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1955–1980, 4th Quart., 2014.

[13] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1617–1634, 3rd Quart., 2014.

[14] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008. [Online]. Available: http://doi.acm.org/10.1145/1355734.1355746

[15] F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network and OpenFlow: From concept to implementation," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2181–2206, 4th Quart., 2014.

[16] A. Lara, A. Kolasani, and B. Ramamurthy, "Network innovation using OpenFlow: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 493–512, 1st Quart., 2014.

[17] S. J. Vaughan-Nichols, "OpenFlow: The next generation of the network?" *Computer*, vol. 44, no. 8, pp. 13–15, 2011. [Online]. Available: http://dblp.uni-trier.de/db/journals/computer/computer44.html#Vaughan-Nichols11

[18] *Software-Defined Networking: The New Norm for Networks*, Open Netw. Found., Palo Alto, CA, USA, Apr. 2012.

[19] S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, Jul. 2013.

[20] K. Kirkpatrick, "Software-defined networking," *Commun. ACM*, vol. 56, no. 9, pp. 16–19, Sep. 2013. [Online]. Available: http://doi.acm.org/10.1145/2500468.2500473

[21] F. de Oliveira Silva, J. H. de Souza Pereira, P. F. Rosa, and S. T. Kofuji, "Enabling future internet architecture research and experimentation by using software defined networking," in *Proc. Eur. Workshop Softw. Defined Netw.*, Oct. 2012, pp. 73–78.

[22] G. Goth, "Software-defined networking could shake up more than packets," *IEEE Internet Comput.*, vol. 15, no. 4, pp. 6–9, Jul. 2011.

[23] M. Karakus and A. Durresi, "A scalability metric for control planes in software defined networks (SDNs)," in *Proc. IEEE 30th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2016, pp. 282–289.

[24] X. Guan, B.-Y. Choi, and S. Song, "Reliability and scalability issues in software defined network frameworks," in *Proc. 2nd GENI Res. Educ. Exp. Workshop*, Mar. 2013, pp. 102–103.

[25] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[26] D. Guha Roy and S. N. Srirama, "A Blockchain-based cyber attack detection scheme for decentralized Internet of Things using software-defined network," *Softw., Pract. Exp.*, vol. 51, no. 7, pp. 1540–1556, Jul. 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.2972

[27] Z. Zeng, X. Zhang, and Z. Xia, "Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT networks," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–10, Feb. 2022.

[28] P. Kamboj and S. Pal, "QoS in software defined IoT network using blockchain based smart contract: Poster abstract," in *Proc. SenSys*, New York, NY, USA, Nov. 2019, pp. 430–431, doi: 10.1145/3356250.3361954.

[29] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *J. Netw. Comput. Appl.*, vol. 143, pp. 167–177, Oct. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519302243

[30] D. B. Rawat, "Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 50–55, Oct. 2019.

[31] H. Al-Sakran, Y. Alharbi, and I. Serguievskaia, "Framework architecture for securing IoT using blockchain, smart contract and software defined network technologies," in *Proc. 2nd Int. Conf. new Trends Comput. Sci. (ICTCS)*, Oct. 2019, pp. 1–6.

[32] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[33] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

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

[35] M. Karakus, E. Guler, and S. Uludag, "QoSChain: Provisioning inter-AS QoS in software-defined networks with blockchain," *IEEE Trans. Netw. Serv. Manage.*, vol. 18, no. 2, pp. 1706–1717, Jun. 2021.

[36] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed, and A. Radwan, "Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things," *IEEE Access*, vol. 9, pp. 139739–139754, 2021.

[37] J. Gao, K. O.-B. O. Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, "A blockchain-SDN-enabled Internet of Vehicles environment for fog computing and 5G networks," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4278–4291, May 2020.

[38] J. Hu, M. Reed, M. Al-Naday, and N. Thomos, "Blockchain-aided flow insertion and verification in software defined networks," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2020, pp. 1–6.

[39] M. J. Islam, A. Rahman, S. Kabir, M. R. Karim, U. K. Acharjee, M. K. Nasir, S. S. Band, M. Sookhak, and S. Wu, "Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3850–3864, Mar. 2022.

[40] K. Kataoka, S. Gangwar, and P. Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 296–301.

[41] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6143–6149, Jul. 2020.

[42] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," *IEEE Access*, vol. 7, pp. 99573–99588, 2019.

[43] A. Rahman, M. K. Nasir, Z. Rahman, A. Mosavi, S. Shahab, and B. Minaei-Bidgoli, "DistBlockBuilding: A distributed blockchain-based SDN-IoT network for smart building management," *IEEE Access*, vol. 8, pp. 140008–140018, 2020.

[44] 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.

[45] N. Rajabi and J. Qaddour, "SDIoBoT: A software-defined Internet of Blockchains of things model," *Int. J. Internet Things*, vol. 8, no. 1, pp. 17–26, 2019.

[46] Q. Shafi and A. Basit, "DDoS botnet prevention using blockchain in software defined Internet of Things," in *Proc. 16th IBCAST*, Jan. 2019, pp. 624–628.

[47] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.

[48] S. A. Latif, S. A. Latif, F. B. X. Wen, C. Iwendi, L.-F. L. Wang, S. M. Mohsin, Z. Han, and S. S. Band, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Comput. Commun.*, vol. 181, pp. 274–283, Jan. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421003662

[49] E. Barka, S. Dahmane, C. A. Kerrache, M. Khayat, and F. Sallabi, "STHM: A secured and trusted healthcare monitoring architecture using SDN and blockchain," *Electronics*, vol. 10, no. 15, p. 1787, Jul. 2021.

[50] S. Hameed, S. A. Shah, Q. S. Saeed, S. Siddiqui, I. Ali, A. Vedeshin, and D. Draheim, "A scalable key and trust management solution for IoT sensors using SDN and blockchain technology," *IEEE Sensors J.*, vol. 21, no. 6, pp. 8716–8733, Mar. 2021.

[51] J. Hu, M. Reed, N. Thomos, M. F. Ai-Naday, and K. Yang, "Securing SDN-controlled IoT networks through edge blockchain," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2102–2115, Feb. 2021.

[52] B. Sellami, A. Hakiri, and S. B. Yahia, "Deep reinforcement learning for energy-aware task offloading in join SDN-blockchain 5G massive IoT edge network," *Future Gener. Comput. Syst.*, vol. 137, pp. 363–379, Dec. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X22002588

[53] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, "Blockchain-based software-defined industrial Internet of Things: A dueling deep Q-learning approach," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4627–4639, Jun. 2019

[54] D. Chattaraj, B. Bera, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing fine-grained access control for software-defined networks using private blockchain," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1542–1559, Jan. 2022.

[55] L. Huo, D. Jiang, S. Qi, and L. Miao, "A blockchain-based security traffic measurement approach to software defined networking," *Mobile Netw. Appl.*, vol. 26, no. 2, pp. 586–596, Apr. 2021.

[56] L. Liu, W. Feng, C. Chen, Y. Zhang, D. Lan, X. Yuan, and S. Vashisht, "BS-IoT: Blockchain based software defined network framework for Internet of Things," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 496–501.

[57] P. M. Bala, S. Usharani, T. A. Kumar, R. Rajmohan, and M. Pavithra, "Blockchain-based IoT architecture for software-defined networking," in *Blockchain, Artificial Intelligence, and the Internet of Things*. Cham, Switzerland: Springer, 2022, pp. 91–115, doi: 10.1007/978-3-030-77637-4.

[58] A. Rahman, M. J. Islam, M. S. I. Khan, S. Kabir, A. I. Pritom, and M. R. Karim, "Block-SDoTCloud: Enhancing security of cloud storage through blockchain-based SDN in IoT network," in *Proc. 2nd Int. Conf. Sustain. Technol. Ind. 4.0 (STI)*, Dec. 2020, pp. 1–6.

[59] S. Faizullah, M. A. Khan, A. Alzahrani, and I. Khan, "Permissioned blockchain-based security for SDN in IoT cloud networks," in *Proc. Int. Conf. Adv. Emerg. Comput. Technol. (AECT)*, Feb. 2020, pp. 1–6.

[60] C. Qiu, F. R. Yu, F. Xu, H. Yao, and C. Zhao, "Blockchain-based distributed software-defined vehicular networks via deep *Q*-learning," in *Proc. 8th ACM Symp. Design Anal. Intell. Veh. Netw. Appl. (DIVANet)*, New York, NY, USA, Oct. 2018, pp. 8–14.

[61] C. Qiu, F. R. Yu, F. Xu, H. Yao, and C. Zhao, "Permissioned blockchain-based distributed software-defined industrial Internet of Things," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–7.

[62] Z. A. E. Houda, A. S. Hafid, and L. Khoukhi, "Co-IoT: A collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN," in *Proc. IEEE GLOBECOM*, Dec. 2019, pp. 1–6.

[63] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, "Cochain-SC: An intra- and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract," *IEEE Access*, vol. 7, pp. 98893–98907, 2019.

[64] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT," *Digit. Commun. Netw.*, Nov. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864822002449

[65] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K.-R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1120–1132, Apr. 2021.

[66] M. Boussard, S. Papillon, P. Peloso, M. Signorini, and E. Waisbard, "STewARD:SDN and blockchain-based trust evaluation for automated risk management on IoT devices," in *Proc. IEEE INFOCOM*, Apr. 2019, pp. 841–846.

[67] J. Luo, Q. Chen, F. R. Yu, and L. Tang, "Blockchain-enabled software-defined industrial Internet of Things with deep reinforcement learning," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5466–5480, Jun. 2020.

[68] A. Muthanna, A. A. Ateya, A. Khakimov, I. Gudkova, A. Abuarqoub, K. Samouylov, and A. Koucheryavy, "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *J. Sens. Actuator Netw.*, vol. 8, no. 1, p. 15, Feb. 2019. [Online]. Available: https://www.mdpi.com/2224-2708/8/1/15

[69] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, and M. S. Hossain, "Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3755–3764, Jun. 2021.

[70] T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," *IEEE Access*, vol. 8, pp. 9146–9156, 2020.

[71] W. Li, W. Meng, Z. Liu, and M.-H. Au, "Towards blockchain-based software-defined networking: Security challenges and solutions," *IEICE Trans. Inf. Syst.*, vol. E103.D, no. 2, pp. 196–203, 2020.

[72] C. Xue, N. Xu, and Y. Bo, "Research on key technologies of software-defined network based on blockchain," in *Proc. IEEE Int. Conf. Service-Oriented Syst. Eng. (SOSE)*, Apr. 2019, p. 2394.

[73] X. Li, Z. Wang, V. C. M. Leung, H. Ji, Y. Liu, and H. Zhang, "Blockchain-empowered data-driven networks: A survey and outlook," *ACM Comput. Surv.*, vol. 54, no. 3, pp. 1–38, Apr. 2021.

[74] S. Wadhwa, H. Babbar, and S. Rani, "A survey on emerging software-defined networking and blockchain in smart health care," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1022, no. 1, Jan. 2021, Art. no. 012056, doi: 10.1088/1757-899x/1022/1/012056.

[75] L. Mastilak, P. Helebrandt, M. Galinski, and I. Kotuliak, "Secure inter-domain routing based on blockchain: A comprehensive survey," *Sensors*, vol. 22, no. 4, p. 1437, 2022.

[76] H. N. Nguyen, H. A. Tran, S. Fowler, and S. Souihi, "A survey of blockchain technologies applied to software-defined networking: Research challenges and solutions," *IET Wireless Sensor Syst.*, vol. 11, no. 6, pp. 233–247, Dec. 2021.

[77] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2017, pp. 303–308.

[78] A. Rahman, A. Montieri, D. Kundu, M. R. Karim, M. J. Islam, S. Umme, A. Nascita, and A. Pescapé, "On the integration of blockchain and SDN: Overview, applications, and future perspectives," *J. Netw. Syst. Manage.*, vol. 30, no. 4, pp. 1–44, 2022.

[79] H. A. Hassan, E. E. Hemdan, W. El-Shafai, M. Shokair, and F. E. A. El-Samie, "A survey on SDN-based intrusion detection systems on the Internet of Thing: Concepts, issues, and blockchain applications," *Wireless Pers. Commun.*, Jul. 2021, doi: 10.21203/rs.3.rs-694000/v1.

[80] F. H. Pohrmen, R. K. Das, W. Khongbuh, and G. Saha, "Blockchain-based security aspects in Internet of Things network," in *Advanced Informatics for Computing Research*, A. K. Luhach, D. Singh, P.-A. Hsiung, K. B. G. Hawari, P. Lingras, and P. K. Singh, Eds. Singapore: Springer, 2019, pp. 346–357.

[81] F. H. Pohrmen, R. K. Das, and G. Saha, "Blockchain-based security aspects in heterogeneous Internet-of-Things networks: A survey," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 10, Oct. 2019, Art. no. e3741.

[82] N. Y.-R. Douha, M. Bhuyan, S. Kashihara, D. Fall, Y. Taenaka, and Y. Kadobayashi, "A survey on blockchain, SDN and NFV for the smart-home security," *Internet Things*, vol. 20, Nov. 2022, Art. no. 100588. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660522000750

[83] S. K. Singh, S. K. Sharma, D. Singla, and S. S. Gill, "Evolving requirements and application of SDN and IoT in the context of industry 4.0, blockchain and artificial intelligence," in *Software Defined Networks: Architecture and Applications*. Hoboken, NJ, USA: Wiley, 2022, ch. 13, pp. 427–496. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119857921.ch13

[84] A. Rahman, J. Islam, D. Kundu, R. Karim, Z. Rahman, S. S. Band, M. Sookhak, P. Tiwari, and N. Kumar, "Impacts of blockchain in software-defined Internet of Things ecosystem with network function virtualization for smart applications: Present perspectives and future directions," *Int. J. Commun. Syst.*, Feb. 2023, Art. no. e5429.

[85] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[86] Y. Abbassi and H. Benlahmer, "BCSDN-IoT: Towards an IoT security architecture based on SDN and blockchain," *Int. J. Electr. Comput. Eng. Syst.*, vol. 13, no. 2, pp. 155–163, 2022.

[87] L. Tran, H. To, L. Fan, and C. Shahabi, "A real-time framework for task assignment in hyperlocal spatial crowdsourcing," *ACM Trans. Intell. Syst. Technol.*, vol. 9, no. 3, pp. 1–26, 2018.

[88] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in *Proc. Int. Conf. Manage. Data (SIGMOD)*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 123–140. [Online]. Available: https://doi-org.libproxy.umflint.edu/10.1145/3299869.3319889

[89] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC)*. New York, NY, USA: Association for Computing Machinery, 2012, pp. 13–16.

[90] B. Negash, A. M. Rahmani, P. Liljeberg, and A. Jantsch, *Fog Computing Fundamentals in the Internet-of-Things*. Cham, Switzerland: Springer, 2018, pp. 3–13.

[91] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *J. Syst. Archit.*, vol. 98, pp. 289–330, Sep. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1383762118306349

[92] H. Ghafoor and I. Koo, "An integrated cognitive radio network for coastal smart cities," *Appl. Sci.*, vol. 9, no. 17, p. 3557, 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/17/3557

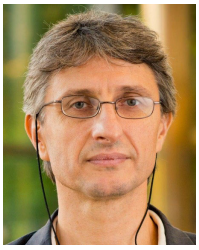
[93] M. S. Mehmood, M. R. Shahid, A. Jamil, R. Ashraf, T. Mahmood, and A. Mehmood, "A comprehensive literature review of data encryption techniques in cloud computing and IoT environment," in *Proc. 8th Int. Conf. Inf. Commun. Technol. (ICICT)*, 2019, pp. 54–59.

[94] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. Boca Raton, FL, USA: CRC Press, 2016.
[95] C. Chio and D. Freeman, *Machine Learning and Security: Protecting Systems With Data and Algorithms*. Sebastopol, CA, USA: O'Reilly Media, 2018.
[96] J. Zhang and D. Tao, "Empowering things with intelligence: A survey of the progress, challenges, and opportunities in artificial intelligence of things," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7789–7817, May 2021.
[97] H. Wu, H. Han, X. Wang, and S. Sun, "Research on artificial intelligence enhancing Internet of Things security: A survey," *IEEE Access*, vol. 8, pp. 153826–153848, 2020.
[98] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.
[99] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100227.
[100] K. Sgantzos and I. Grigg, "Artificial intelligence implementations on the blockchain. Use cases and future applications," *Future Internet*, vol. 11, no. 8, p. 170, Aug. 2019.
[101] A. A. Hussain and F. Al-Turjman, "Artificial intelligence and blockchain: A review," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 9, 2021, Art. no. e4268.
[102] M. Latah and L. Toker, "Artificial intelligence enabled software-defined networking: A comprehensive overview," *IET Netw.*, vol. 8, no. 2, pp. 79–99, Mar. 2019.
[103] 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.
[104] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the age of machine learning and software-defined networking," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4829–4842, Dec. 2018.
[105] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 393–430, 1st Quart., 2019.
[106] D. T. Tuan, P. T. Duy, L. C. Hau, and V.-H. Pham, "A blockchain-based authentication and access control for smart devices in SDN-enabled networks for metaverse," in *Proc. 9th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Oct. 2022, pp. 123–128.
[107] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 319–352, 1st Quart., 2023.
[108] W. Y. B. Lim, Z. Xiong, D. Niyato, X. Cao, C. Miao, S. Sun, and Q. Yang, "Realizing the metaverse with edge intelligence: A match made in heaven," *IEEE Wireless Commun.*, early access, Jul. 4, 2022, doi: 10.1109/MWC.018.2100716.
[109] J. Singh, G. Singh, and A. Verma, "The anatomy of big data: Concepts, principles and challenges," in *Proc. 8th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2022, pp. 986–990.
[110] N. Aljehane, "Big data analytics: Challenges and opportunities," in *Proc. Int. Conf. Comput. Inf. Technol. (ICCIT)*, Sep. 2020, pp. 1–4.
[111] E.-K. Hong, I. Lee, B. Shim, Y.-C. Ko, S.-H. Kim, S. Pack, K. Lee, S. Kim, J.-H. Kim, Y. Shin, Y. Kim, and H. Jung, "6G R&D vision: Requirements and candidate technologies," *J. Commun. Netw.*, vol. 24, no. 2, pp. 232–245, Apr. 2022.
[112] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.
[113] L. Zhang, M. Peng, W. Wang, Z. Jin, Y. Su, and H. Chen, "Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 10, Oct. 2021, Art. no. e4315. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4315
[114] S. Luo, H. Li, Z. Wen, B. Qian, G. Morgan, A. Longo, O. Rana, and R. Ranjan, "Blockchain-based task offloading in drone-aided mobile edge computing," *IEEE Netw.*, vol. 35, no. 1, pp. 124–129, Jan. 2021.
[115] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konecný, S. Mazzocchi, B. McMahan, T. V. Overveldt, D. Petrou, D. Ramage, and J. Roselander, "Towards federated learning at scale: System design," in *Proc. Mach. Learn. Syst.*, vol. 1, 2019, pp. 374–388.
[116] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020.

STEPHEN W. TURNER (Member, IEEE) received the B.S. degree in computer science and applied mathematics from Western Michigan University, in 1987, and the M.S. and Ph.D. degrees in computer science from Michigan State University, East Lansing, MI, USA, in 1989 and 1995, respectively. He is currently an Associate Professor in computer science with the University of Michigan-Flint. He is also the Leader of the Research Cluster on Urban Sustainability and Environmental Health. His research interests include security, smart grids, EV charging strategies for intelligent transportation systems, and better pedagogical approaches through next-generation digital learning environment.

MURAT KARAKUS received the B.S. degree in mathematics from Suleyman Demirel University, Turkey, in 2009, the M.S. degree in computer science and information systems from the University of Michigan-Flint, USA, in 2013, and the Ph.D. degree in computer science from the Purdue School of Science, Indianapolis, USA, in 2018. He is currently an Assistant Professor with Ankara University, Turkey. He has more than 20 peer-reviewed publications and serves as a reviewer for esteemed IEEE, ACM, and Elsevier journals and conferences. His current research interests include next-generation network architectures, such as software-defined networking (SDN), blockchain technology, network scalability, quality of service (QoS), routing, the economic analysis of network architectures and designs, and pricing network services. He was a recipient of the Best Paper Award at ACM SIGITE 2011 Conference.

EVRIM GULER received the Ph.D. degree in computer science from Georgia State University, Atlanta, GA, USA, in 2019. He is currently an Assistant Professor with the Department of Computer Engineering, Bartin University, Turkey, where he leads the Distance Education and Research Center. His research interests include elastic optical networks, software-defined networking, network function virtualization, blockchain, routing, smart systems, and network modeling.



SULEYMAN ULUDAG (Member, IEEE) is currently a Professor in computer science with the University of Michigan-Flint. His research interests include secure data collection, smart grid communications, smart grid privacy, smart grid optimization, demand response bidding privacy, denial-of-service in the smart grids, cybersecurity education and curriculum development, routing and channel assignment in wireless mesh networks, quality-of-service (QoS) routing in wired and wireless networks, and topology aggregation. He received the Fulbright U.S. Scholar Program Core Award, in 2012 and 2018.