Journal of Network and Systems Management (2022) 30: 73
https://doi.org/10.1007/s10922-022-09682-4

# On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives

**Anichur Rahman[1] · Antonio Montieri[2] · Dipanjali Kundu[1] · Md. Razaul Karim[3] · Md. Jahidul Islam[4] · Sara Umme[1] · Alfredo Nascita[2] · Antonio Pescapé[2]**

Received: 1 December 2021 / Revised: 16 June 2022 / Accepted: 1 August 2022 /
Published online: 6 September 2022


## Abstract

Blockchain (BC) and software-defined networking (SDN) are leading technologies which have recently found applications in several network-related scenarios and have consequently experienced a growing interest in the research community. Indeed, current networks connect a massive number of objects over the Internet and in this complex scenario, to ensure security, privacy, confidentiality, and programmability, the utilization of BC and SDN have been successfully proposed. In this work, we provide a comprehensive survey regarding these two recent research trends and review the related state-of-the-art literature. We first describe the main features of each technology and discuss their most common and used variants. Furthermore, we envision the integration of such technologies to jointly take advantage of these latter efficiently. Indeed, we consider their group-wise utilization—named BC–SDN—based on the need for stronger security and privacy. Additionally, we cover the application fields of these technologies both individually and combined. Finally, we discuss the open issues of reviewed research and describe potential directions for future avenues regarding the integration of BC and SDN. To summarize, the contribution of the present survey spans from an overview of the literature background on BC and SDN to the discussion of the benefits and limitations of BC–SDN integration in different fields, which also raises open challenges and possible future avenues examined herein. To the best of our knowledge, compared to existing surveys, this is the first work that analyzes the aforementioned aspects in light of a broad BC–SDN integration, with a specific focus on security and privacy issues in actual utilization scenarios.

**Keywords** Blockchain · Software defined networking · BC–SDN integration · Security · Privacy · Confidentiality · Internet of Things

✉ Antonio Montieri
antonio.montieri@unina.it

Extended author information available on the last page of the article

## 1 Introduction

With the growing amount of always-online connected devices, the challenges to face within modern network environments have also grown. It is estimated that nowadays 30 billion devices are connected over the Internet and this number will reach 75 billion worldwide by 2025 [1]. This increase of devices is creating a massive number of issues such as attacks against the networking systems, data theft, addressing issues, sensors' energy consumption and battery loss, etc. Moreover, after the revolution of Industry 3.0 and 4.0 [2], the Internet is no longer only a medium to exchange files or emails but it is the enabler of several safety-critical operations which makes these issues much more urgent. Thus, the handling of such safety-critical operations must be carried out to properly utilize the data generated by several devices interconnected over the network [3].

Software-defined networking (SDN) is an interesting paradigm that can be used to enhance and manage various security aspects in modern networks such as Internet of Things (IoTs) environments. For instance, to provide better system security, it is necessary to permit the use of resources only among authorized users [4]. This limits the possibility that third-party users get control over the system and lowers the frequency of attacks [5]. Further, the large number of connected devices creates a huge amount of data passing from one system segment to another, producing enormous traffic in turn. As conventional networking devices such as routers or switches have to make choices and then monitor the traffic flow, the overall speed of operations is slower. In this sense, the SDN paradigm with the OpenFlow protocol allows the SDN controller to link to other devices and separates hardware from software [6]. Indeed, the SDN controller can incorporate a constructive or reactive mechanism to remove or even change the traffic flow via a flow table. The transmitted traffic is then handled in the so-called control layer [7], which can also protect the networking devices from internal and external attacks.

Blockchain (BC) is another technology that can be a possible solution to enforce a verification system at every edge and handle trust-management issues to make the system robust against various attacks [8] and to ensure block validation using encryption or consensus mechanisms [9]. BC provides a peer-to-peer (P2P) communication system that maintains a database for all members of the network where every record about the connection establishment is easily stored and properly maintained. In addition, the chain of blocks can not be easily modified: changes are possible when proper validation is ensured, and only in this case a new block can be included in the BC [10]. Furthermore, it ensures authenticity and confidentiality to the data transmitted among network nodes.

Given the high interest that BC and SDN technologies have generated in the research community (and more recently also in the industry), our research aims to provide insights and guidelines to foster their fruitful integration (i.e. BC–SDN). More specifically, in this survey, we seek answers to the following research questions:

**RQ1.** **BC–SDN Ecosystem:** What are the key features and benefits of the BC–SDN integration as investigated in state-of-art works?

**RQ2.** **Security and Privacy in BC–SDN:** Which are the main security and privacy threats affecting BC and SDN? How have they been faced in literature by exploiting the integration of both technologies?

**RQ3.** **Application of BC–SDN:** Which are the most relevant applications that can benefit from BC–SDN?

**RQ4.** **Future Challenges:** What are the challenges to deal with in the near future for integrating BC–SDN with emerging technologies in computational intelligence?

### 1.1 Related Surveys

The present survey discusses essential information related to both SDN and BC considering also their security and privacy aspects as well as their applications. In the last years, many works have focused on these technologies proving that they are heavily attracting the interest of the research community. Hereinafter, we review the most recent surveys (published within the last 5 years) regarding such technologies and their integration, briefly discussing the aspects on which each work is focused.[1]

*SDN.* In [37], the authors discuss the 5G network softwarization and slicing strategy based on SDN and network function virtualization (NFV) technologies. Different industrial initiatives and projects, their requirements, and various architectural approaches for 5G networks are also described. Similarly, Bannour et al. [38] focus on the SDN approach and particularly on distributed SDN controllers. Improving the security of the SDN environment and especially of SDN controllers is the main topic of the work in [39]. Additionally, Bizanis and Kuipers [40] propose the joint utilization of SDN and network virtualization technologies to bring several functionalities to IoT applications. In [41], a brief discussion on SDN control plane focusing on scalability issues is presented. The authors also develop different controller design schemes such as flat, hierarchical, and hybrid controllers. Furthermore, in [42], the authors present a strategy for smart homes using SDN that ensures the privacy of the system. The authentication of user is accomplished by encryption procedure based on a symmetric key protocol. In another SDN–IoT integration-based work [43], the authors suggest to integrate SDN and IoT to develop an intelligent framework that is capable of providing solutions to different problems related to Industry 4.0 applications that have arisen during the COVID-19 pandemic.

[1] When a work covers different technologies, we categorize it based on its main topic.

*Blockchain.* Tariq and al. [44] propose to leverage BC to manage several applications such as Wireless Sensor Networks, Vehicular Ad hoc Networks (VANETs), IoT, and healthcare systems. They review the existing problems, their solutions, and possible security issues. Besides, Deepa et al. [45] integrate these studies presenting different approaches for potential integration of Big Data applications with BC technology. More recently, the survey in [46] discusses different case studies of practical usage of BC for healthcare data management systems. The integration of BC within IoT systems is analyzed in [47] where the authors propose the definition of Blockchain of Things to name the synthesis of BC into 5G and industrial applications. Also, the survey in [21] focuses on the management of information system using BC with particular attention on the security issues. Similarly, Bhutta et al. [22] present the evolution of BC technology along with the specific security measures introduced, while Hewa et al. [23] discuss the technical aspects of BC focusing on its future scopes.

*Integration of BC and SDN.* Wadhwa et al. [48] investigate healthcare systems enriched with the integration of BC and SDN. They describe various use cases where the benefits of these two technologies can be fruitfully leveraged. With a specific eye on security, in [49], the authors discuss SDN-based intrusion detection systems (IDSs) in BC applications. Likewise, Alharbi [50] takes into account BC to protect the SDN environment, also assessing the feasibility of this powerful integration.

For the sake of completeness, other related surveys on BC and SDN—not detailed in the present subsection for brevity—are reported in Table 1, which groups them based on the related technology and summarizes the main topics covered by each work.

*Positioning of Our Survey.* In the present survey, we aim to investigate the integration of BC and SDN technologies with an eye on security and privacy issues in real applications. To the best of our knowledge, this study is the first survey that takes into account BC and SDN technologies by providing details on both their main features and deepening their effective integration along with actual use cases. As reported in previous paragraphs and further summarized in Table 1, we analyze in a systematic manner different aspects scattered across previous works. Indeed, unlike the works investigating the application of BC or SDN alone, we firstly provide an overview of BC and SDN applications underlining their security and privacy aspects, then we discuss the BC–SDN integration by analyzing the peculiarities and (security) issues deriving from it. In this regard, comparing our survey with recent ones covering BC–SDN [48–50], (i) we expressly make BC–SDN the main pillar of our investigation (differently than [49]) and we do not narrow our dissertation to (ii) specific use cases (e.g., healthcare [48]) or (iii) particular aspects of interest (e.g., implementation feasibility [50]).

### 1.2 Contributions and Organization of the Survey

In this work, we discuss SDN and BC leading technologies and their fruitful integration. In detail, we provide an extensive analysis of their features, security and

**Table 1** Related surveys regarding SDN and BC

| Tech | Reference | Year | Main topic |
|---|---|---|---|
| SDN | [11] | 2021 | Solutions to cyber defence on SDN based systems with taxonomy |
| | [12] | 2021 | Security and Privacy concerns of Controllers of SDN |
| | [13] | 2021 | SDN based Security for 5G framework |
| | [14] | 2021 | Survey of Solution to DDoS and DoS attack in SDN |
| | [15] | 2021 | SDN-based systematic review for edge and cloud computing in IoT |
| | [16] | 2021 | SDN framework for smart industrial IoT environment |
| | [17] | 2019 | Integration of SDN and Smart Building |
| | [18] | 2019 | Application of SDN for improving security in computer networks |
| | [19] | 2018 | SDN–NFV framework for ensuring security in IoT environment |
| | [20] | 2018 | Security aspects and open challenges of SDN technology |
| BC | [21] | 2021 | Management and Improvement of information systems security using BC |
| | [22] | 2021 | Analysis of the evolution, security of the BC technology |
| | [23] | 2021 | Aspects of BC with future research scopes |
| | [24] | 2021 | A survey of the application of BC specifically in decentralization method |
| | [25] | 2021 | BC for addressing challenges and security aspects in IIoT |
| | [26] | 2021 | Integration of IoT and BC for enhancing security |
| | [27] | 2020 | Improvements in Industry 4.0 by integrating BC technology |
| | [28] | 2020 | Approaches for enhancing security in BC technology |
| | [29] | 2020 | Security issues of IoT and solutions provided by BC technology |
| | [30] | 2019 | Classification of security vulnerabilities in BC technology |
| | [31] | 2019 | Privacy issues associated with BC-based applications |
| | [32] | 2018 | Applications and challenges of BC for IoT and other paradigms |
| | [33] | 2018 | Proof- and voting-based algorithms for consensus in BC technology |
| | [34] | 2018 | BC-based approaches for different security services |
| | [35] | 2018 | Overview of BC technology and classification of its threat models |
| | [36] | 2018 | BC-based security techniques designed for, or applicable to IoT |

The works are grouped based on the related technology and reported in reverse chronological order within each group

privacy issues, and applications. Finally, we discuss open challenges and future perspectives. We also consider valuable benefits achieved with the integration of these technologies in order to better support applications in many fields. To summarize, in this survey, we offer the following contributions:

- We discuss the state-of-art literature and provide a general overview about BC and SDN.
- We present the effective benefits of the integration of SDN with BC; we also investigate its existing and upcoming features.
- We discuss security and privacy issues of BC and SDN and their integration (i.e. BC–SDN).
- We review the applications of these technologies in different fields.

- Finally, we describe issues, open challenges, and future investigations related to considered technologies.

In view of these aims, we review recent papers related to BC and SDN, and their integration by considering state-of-art proposals (with related motivations) and focusing on their features and benefits, as well as security and privacy concerns. Moreover, we review articles related to real application scenarios of BC–SDN as an extension of their individual application fields. In particular, we have selected such studies prioritizing more relevant ones (i.e. those deepening security and privacy aspects or describing actual use cases) published in the last five years (see e.g. Table 3).

The remainder of this survey is organized as follows: Sect. 2 presents a general overview of analyzed technologies (i.e. BC and SDN). Section 3 introduces the motivations behind the BC–SDN integration also reviewing state-of-art proposals. The security and privacy issues in BC and in the aforementioned integration are discussed in Sect. 4, Successively, the applications of BC and BC–SDN are presented in Sect. 5. Furthermore, in Sect. 6, we focus on the current research challenges and future directions for the effective employment of considered technologies. Finally, we conclude the survey in Sect. 7. To ease readers, Fig. 1 depicts the road map of the present survey. Also, Table 2 summarizes the acronyms used in the text for readability.

## 2 Background Overview

This section focuses on some key aspects of BC and SDN providing an useful overview of these technologies. Section 2.1 describes different types of BC, its key aspects, and methods for attaining consensus in transactions. In Sect. 2.2, the SDN paradigm is discussed, describing the properties of the three planes (i.e. data, control, and application) SDN is made of.

### 2.1 Blockchain

BC technology was firstly introduced by Satoshi Nakamoto (pseudonym) in 2008 and it is currently exploited in numerous applications. A BC is a decentralized and distributed ledger and every participant can authenticate it without the interference of any central authority or special individual which provides a clearinghouse service verifying and clearing all transactions. Therefore, the BC is assembled independently by every node in the network. Each *block* records some or all most recent transactions that have not been recorded in a previous block. As shown in Fig. 2, each block consists of (i) the block header encompassing current and prior cryptographic block hash values, a timestamp, and a nonce; (ii) the main body encompassing transaction hash value, sender and receiver identity, and signature for each transaction. The users who share their computing power to verify if the transactions in the blocks are legitimate in exchange for a reward are called *miners*. They have to

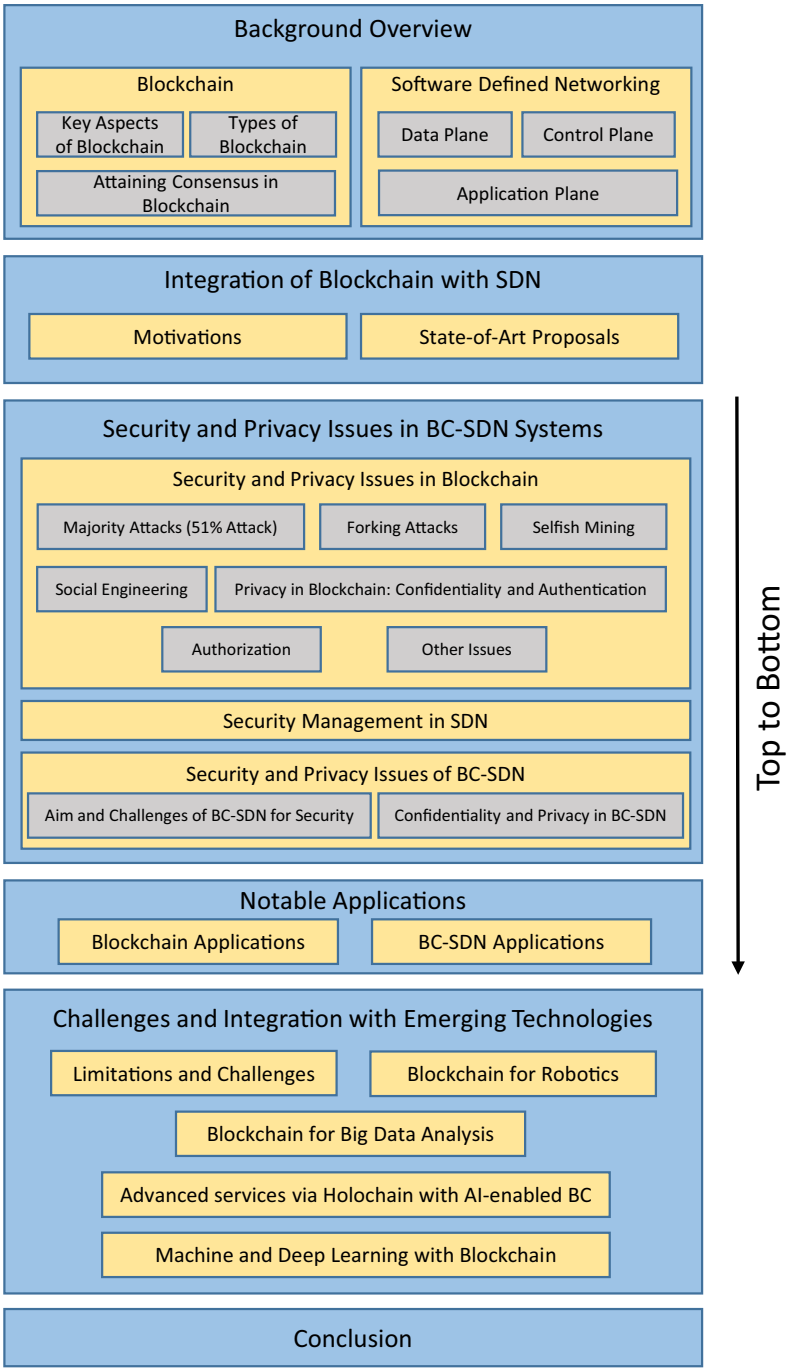



**Fig. 1** Road map of the present survey

**Table 2** List of acronyms in alphabetical order

| Acronym | Definition |
|---|---|
| *ACL* | Access Control List |
| *AI* | Artificial Intelligence |
| *API* | Application Programming Interface |
| *BC* | Blockchain |
| *DDoS* | Distributed Denial of Service |
| *DL* | Deep Learning |
| *IDS* | Intrusion Detection System |
| *ML* | Machine Learning |
| *NFV* | Network Function Virtualization |
| *P2P* | Peer to Peer |
| *PoS* | Proof of Stake |
| *PoW* | Proof of Work |
| *SC* | Smart Contract |
| *SDN* | Software-Defined Networking |
| *SPBFT* | Simplified Practical Byzantine Fault Tolerance |
| *VANET* | Vehicular Ad hoc Network |

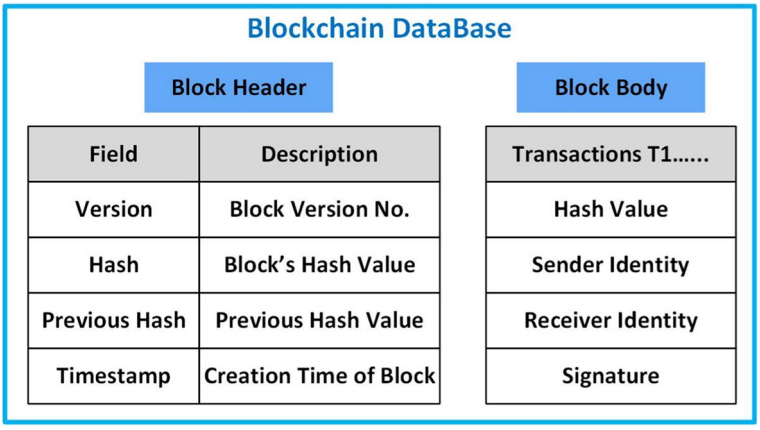



**Fig. 2** Structure of each block constituting a Blockchain

resolve a statistical problem based on the calculation of a cryptographic hash function to confirm the latest transactions and list all of them within the global ledger. Normally, a block is extracted every 5 to 10 min.

The newly mined block is attached to the BC once the majority of its participants agree that it is valid; in other words, adding a new block requires to reach a *consensus* among the miners (also called nodes in this context). More specifically, the consensus is an artifact of the asynchronous interaction of thousands of independent nodes, all following simple rules. The most common consensus algorithms are the *Proof of Work (PoW)* and the *Proof of Stake (PoS)* in which the miners needs to

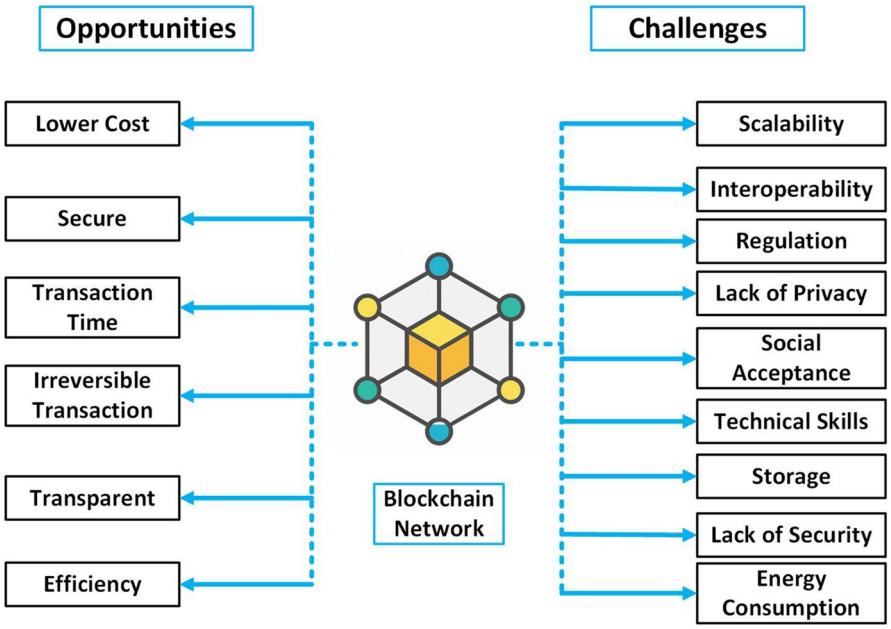



**Fig. 3** Opportunities and challenges in Blockchain network

provide a certain proof that must be validated by other nodes in the network to be allowed to publish (cf. Sect. 2.1.3).

It is worth underlining that blocks can only be added and not modified. Indeed, after a block is added to the BC, modifying data in a block of the chain is an extremely challenging task because it requires changing all of the following blocks. Therefore, the BC ledger becomes more and more immutable as time passes.

To summarize, in Fig. 3, we provide a diagram reporting the opportunities (shown on the left side) and the related challenges (shown on the right side) related to the utilization of the BC technology. We can notice that if on the one hand, the opportunities and advantages of utilizing the BC are enormous, on the other hand obstacles and challenges must be carefully considered and mitigated to fully exploit BC potential especially in dynamic and controllable environments (as for instance in software-defined networks).

### 2.1.1 Key Aspects of Blockchain

Hereinafter, we describe the main features that characterize a generic BC.

*Decentralization.* BC has a distributed and decentralized structure [51] where there is no central node or trust authority to store data or determine the transaction validity and order. Moreover, BC does not apply any set of rules to establish the transactions or regulating the way nodes interact. Otherwise, consensus is reached via the interplay of thousands of independent nodes independently verifying a set of criteria.

*Transparency.* BC is transparent in recording new data and also in updating them because the system itself validates and authenticates transactions. Third party or malicious users can not include fake transactions into the ledger.

*Autonomy.* The main objective of BC is to switch the trust from one centralized authority to the asynchronous network of nodes [52]. As discussed before, based on the consensus algorithm, every node can transfer and securely update data without any interference.

*Immutability.* Records are immutably stored forever in blocks unless someone tries to alter them. Indeed, the consensus mechanism is theoretically vulnerable to attacks by miners attempting to use their hashing power to malicious ends. Indeed, if a miner acting as an attacker or intruder can control the majority (i.e. 51%) of the total network mining power, he can attack the consensus mechanism so as to disrupt the security and availability of the BC. For instance, an attacker can cause previously confirmed blocks to be invalidated by forking below them and re-converging on an alternate chain [53]. Actually, given the massive increase of total hashing power, this possibility is almost zero also for a pool of malicious miners.

*Anonymity.* One of the key characteristics of BC is that it allows the users to perform pseudonymous transactions that are also verifiable and thus trusted. Firstly, BC users are identified via a public address which does not contain any identifiable information to tie the address or the user. Also, BC solves the trust issue from node to node. When a node transfers data or (crypto-)money toward another node, no one traces the origin and other nodes: all the details remain hidden and are recorded into the ledger.

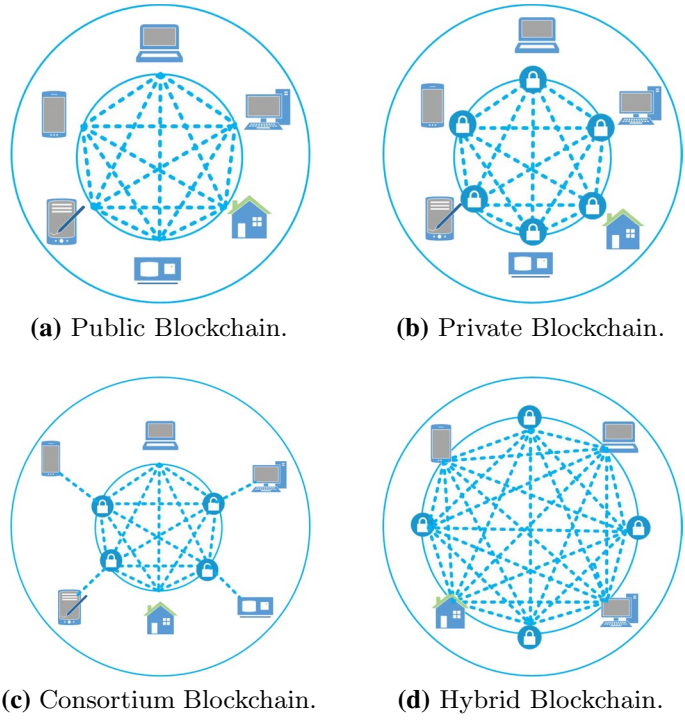
*Open Source Implementation.* Several BC open-source projects have been launched in the open-source community since BC inception. Open source BC platforms enable autonomous developers to create decentralized applications based on BC technology which can be exploited by every interested user and are characterized by publicly verified records.

### 2.1.2 Types of Blockchain

In the following, we discuss four different categories in which BC technologies can be divided based on their structural characteristics.

*Public Blockchain.* A public BC is fully open source. Anyone can participate as a user, developer, or community member, without restrictions on new participants. Figure 4a sketches the structure of a public BC and shows the end users and their connections. All of them are acting as a block of the public ledger. The general user can have different nature and computational capabilities (e.g., a server or a smartphone user). A public BC is also transparent because each member can independently access transaction details and control how the state of the BC evolves, and it is fully decentralized because no one centrally regulates the transactions. Also, anyone can join the public BC network regardless of location or nationality, and the authorities can hardly shut down the accounts given their (pseudo-)anonymity. Common examples of public BCs are Bitcoin, Ethereum, and Litecoin.

*Private Blockchain.* A private BC is characterized by a single organization which has the sole control over the rules of the BC. Therefore, the participation is



**(a)** Public Blockchain. **(b)** Private Blockchain.

**(c)** Consortium Blockchain. **(d)** Hybrid Blockchain.

**Fig. 4** Types of Blockchain

restricted by the authority which is in charge of managing and accessing the data. Figure 4b depicts the structure of a private BC. The central web-like structure is the representation of the logical connectivity of the blocks. Unlike the public one, the private BC has restrictions on the access of the transactions and related information. Private BCs are indeed meant for a company who would like to collaborate and promote data but does not want that sensitive information is exposed on the public BC. The entities operating in private BCs have full control of members and governance systems. Commonly, private BCs have a token associated with the chain and are used in supply chain management, digital identity, vote counting, asset ownership, Hyperledger, etc. Given its more centralized nature, for most applications, a private BC could replace a decentralized database. Moreover, a private BC can be also used for educational purposes.

*Consortium Blockchain.* A consortium BC has a selected group of participants (e.g., several organizations) called *consortium* or *federation*, which cooperate with the aim of taking advantage from BC capabilities (e.g., defining a system to reach consensus between organizations). Figure 4c shows the general structure of a consortium BC. The major advantage of this type of BC over a private BC is that it depends on (and is managed by) several organizations instead of only one. Users in the consortium can operate or run a node, can make transactions, and audit the BC. Commonly, participants can be individuals coming from banks, government,

or supply chain management systems. Common examples of consortium BCs are Hyperledger and Corda.

*Hybrid Blockchain.* A hybrid BC tries to exploit the best aspects of the other types of BC (i.e. public, private, and consortium) to overcome their weaknesses and provide an efficient solution for trustworthy data sharing, access management, etc. Figure 4d outlines the structure of a hybrid BC. As shown in the figure, the blocks could be both restricted or public. Thus, an authority can make the transaction ledger available to the users based on their needs. With this type of BC, it is simpler to operate the business thanks to its functionalities that also preserve security and privacy. Indeed, it is more flexible and transparent for the business purpose to keep the data private and allows to decide what portion of data shall be made public. Nowadays, hybrid BCs are mainly used for data protection as in IoT networks and supply chain management systems.

### 2.1.3 Attaining Consensus in Blockchain

As discussed above, consensus algorithms are of paramount importance in a BC: they are used to decide how a new block is verified and added to the chain. Hereinafter, we discuss two common types of consensus algorithm: proof-based and voting-based [33].

*Proof of Work (PoW).* PoW is a proof-based consensus algorithm in which miners need to prove that they have done a certain amount of computing work to be allowed to publish. In detail, the PoW is included in a new block and acts as proof that the miner spent significant computing effort. PoW requires to solve a complex mathematical problem [54] based on a hash-cryptography puzzle. The latter needs significant computational power to be solved but its solution can be quickly verified. Miners compete each other for accomplishing this task, and when a miner obtains a solution, the latter is broadcast to the network. All other miners then verify if the solution is correct, and in this case the new block is added to the chain. The competition to solve the PoW algorithm to earn reward and the right to record transactions on the BC is the basis for BC security model [53]. For instance, PoW can be used to prevent cyber-attacks such as Distributed Denial-of-Service (DDoS) that would be inefficient since the cost incurred for exhausting BC resources via the DDoS would be significantly greater than the potential rewards for attacking the network.

*Proof of Stake (PoS).* PoS is a proof-based consensus algorithm mainly used in public BC, which aims to overcome the unfairness of PoW. Indeed, the latter favors miners having more powerful equipment, which can thus find a suitable solution to the cryptography puzzle easier than other miners with less powerful equipment. More specifically, PoS is based on the idea that a miner who owns much stake (i.e. the percentage of coins held) would be more trustful. PoS is considered as less risky in terms of revenue for miners to attack the network, as it structures compensation in a way that makes an attack less advantageous for a malicious miner.

*Voting-based Consensus.* Voting-based consensus algorithms presume that the nodes should be known, in contrast to proof-based algorithms where nodes can freely join or leave the network. Therefore, they are more suited to private or consortium BCs. Furthermore, the nodes have to both maintain the ledger (as in

proof-based) and jointly verify new blocks via a voting mechanism (differently than proof-based). Each node communicates with other nodes to decide if adding the new block to the chain: a certain number of nodes (depending on the specific voting mechanism) have to verify the same proposed block before validation.

### 2.2 Software Defined Networking

In conventional systems, network connections are established via switches and routers, which are also responsible for transmitting data over the network. Such a networking scheme may be subject to lack of confidentiality and then could be prone to third-party attacks. For these reasons, the development of the SDN paradigm is crucial. SDN is a networking strategy that efficiently provides the facility of a centralized environment and aims to decouple data transfer process from the devices designed for it [6]. This paradigm is based on the existence of different *planes*, each responsible for some specific functions: (i) the data plane is responsible for packet forwarding, (ii) the control plane decides on routing using a flow table containing rules to properly manage incoming packets, and (iii) the application plane encompasses the services made available to the users. It is worth noting that flow rules can be easily changed according to the needs [55] by exploiting the improved programmability and control provided by SDN compared to conventional networking systems [56]. OpenFlow is the most known protocol used for the communication between the switches and the central controller in SDN environments (despite it still has some vulnerabilities [57]). Figure 5 depicts the structure of a common SDN architecture, whose planes and related interconnections are described hereinafter.

*Data Plane.* The data plane (also known as edge or infrastructure plane as reported in Fig. 5) is the lowest plane of an SDN architecture and comprises the devices used for data forwarding such as switches (physical or virtual), access points, routers, etc. The communication between the data plane and the control plane is established with the OpenFlow protocol through the *Southbound application programming interface (API)* commonly using encrypted channels. The data plane performs packet forwarding based on the flow rules providing forwarding logic, which are defined according to the OpenFlow specification and installed through the Southbound API by the control plane [58]. Flow rules include MAC and IP destination addresses, transport-layer source and destination ports, and other necessary information for matching the desired packets. Notably, OpenFlow rules can be exploited to implement firewalls and enforce various security policies.

*Control Plane.* The control plane is the middle (viz. backbone) plane in an SDN architecture. It is considered as the brain of the networking system [55] and is in charge of managing the routing process. In more detail, the control plane encompasses logic and functional controllers applied to manage the control logic at different levels and to provide controlling functionalities, respectively. As shown in Fig. 5, its core can be realized via different OpenFlow-compliant implementations (e.g., NOX, POX, Beacon, Floodlight, etc.) [41]. It is connected with the application plane through the *Northbound API* and with data plane through the *Southbound API*. Additionally, two other interfaces are the *Eastbound API* and the *Westbound*

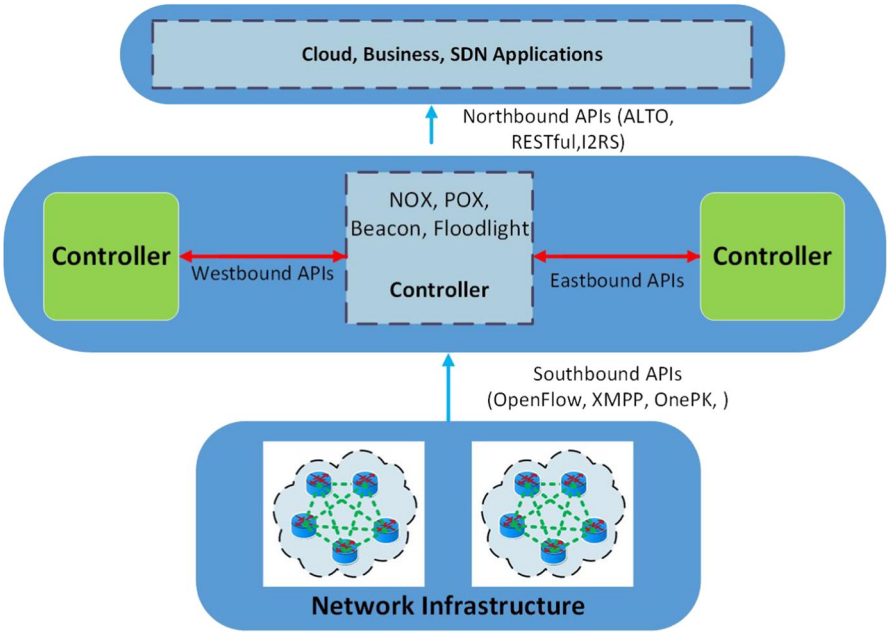



**Fig. 5** General SDN architecture

*API* used for the communication between multiple distributed controllers [59]. It is worth noticing that the control plane provides several enhanced network services which offer improved management, QoS, and data privacy and security to the network infrastructure.

*Application Plane.* The application plane is the topmost plane of an SDN architecture. It includes programs to control the networking system and establishes a connection with the control plane using the *Northbound API* (usually a RESTful API). It also provides higher-level services to the SDN users and applications running on top of existing controller platforms. In detail, from this plane, applications transmit their requirements to the SDN controller where they are processed and then translated into commands and rules for the data plane devices of the SDN architecture. Some of the most common SDN applications are routing, load balancing, and firewalling [38].

## 3 Integration of Blockchain with SDN

This section describes the integration of SDN and BC technologies, whose fundamentals have been provided in Sect. 2. Figure 6 depicts a common scenario in which both public and private BCs are integrated in a multi-domain network defined via the SDN paradigm. Each domain uses a distinct SDN controller, which communicates with the others via a P2P connection. Specifically, Sect. 3.1 reports reasons why researchers have proposed this integration and Sect. 3.2 collects state-of-art

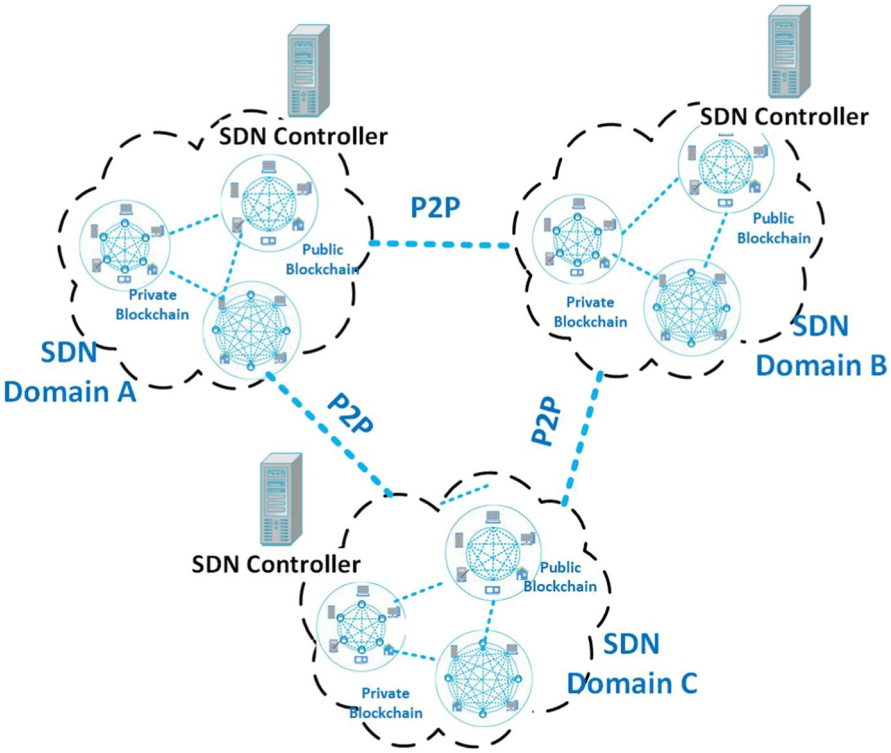



**Fig. 6** Example of the integration of Blockchain with SDN

proposals. We point the interested reader to the specific works reviewed hereinafter, each proposing a particular realization of the general scenario exemplified in Fig. 6 to fulfill the different needs (e.g., reducing latency, optimizing resource usage, guaranteeing security and privacy) of considered application scenarios.

### 3.1 Motivations

In modern networks (e.g., always online smartphones, IoT sensors), the enormous number of interconnected devices produces a considerable amount of data gathered from the actual world. In this scenario, a urgent need to properly manage data arises and SDN is proposed as a solution because it can programmatically handle all the data received from the network environment [60]. Altering the base architecture of a network system is a challenging task; SDN makes it much easier and allows to quickly modify network characteristics. Researchers are prompted to take advantage of the capabilities of the SDN paradigm that can be exploited to performs distinct operations on the data based on the specific layer on which they operate [61].

Unfortunately, the communication among SDN planes is not fully secured and hence its adoption could lead to a corrupted network system due to maliciously

wrong information exchanged [62]. To enhance the security and reliability of SDN networks, BC could efficiently help in checking the authenticity of transmissions [63–65]. Moreover, the addition of smart contracts (SCs) into the BC validation process makes this technology even more trustworthy [66]. Besides, BC keeps the history of transaction in an immutable ledger that can prevent any third party interaction and tampering. However, on the one hand, BC can take the responsibility of the security of data transmission but on the other hand, it can not manage the data from IoT directly. Therefore, the integration of SDN and BC has been pursued to jointly take advantage of the peculiarities of both technologies.

### 3.2 State-of-Art Proposals

We now discuss the research works that have proposed the joint usage of BC and SDN. Many researchers have suggested different BC–SDN architectures to guarantee latency, network performance, resource usage, security, and other desirable features [67–73]. In the following, we go into details of such works.

Xie et al. [74] leverage SDN for 5G VANETs and show that their BC-based IoT network can unveil malicious vehicular nodes and messages. Similarly, Zhang et al. [70] also introduce a distributed BC-based software-defined VANET framework for smart cities named *Block-SDV*. In detail, Block-SDV integrates a novel deep Q-learning approach to solve the optimization problem of finding the optimal features for BC (e.g., trust features of BC nodes, number of consensus nodes, trust features of each vehicle, and computational capability of BC). The effectiveness of Block-SDV and related deep Q-learning is demonstrated in a simulation environment. Gao et al. [75] present a trust-based model to detect malicious activities integrating BC and SDN to improve security in 5G and fog VANET networks. The joint adoption of BC and SDN technologies have been also exploited for the design of IDSs employed in the control framework of industries [72]. El Houda et al. [68] propose a BC-based architecture named *Cochain-SC*, having two levels of attack mitigation: intra-domain and inter-domain DDoS mitigation in SDN. More specifically, the combination of intra entropy-based, intra Bayes-based, and intra-domain mitigation schemes is used to classify and mitigate the impact of malicious traffic. Furthermore, for inter-domain, the authors introduced an SC-based architecture that considered Ethereum technology to simplify the collaboration among SDN-based autonomous systems against DDoS attacks. Finally, the performance of their proposal is assessed based on efficiency, flexibility, security, and cost effectiveness.

Sharma et al. [67] propose the *DistBlockNet* architecture that allows the cooperation of SDN and BC in an IoT network. The authors devise a strategy for updating and formalizing the flow rule table applying a BC, and evaluate the performance according to various metrics showing better results compared to previous works. Rahman et al. [61] present *DistBlockBuilding*, a distributed BC–SDN architecture for smart cities, designing also a cluster-head selection algorithm for collecting sensors data with low energy dissipation. The authors evaluate the performance with different parameters such as throughput, latency, and packet arrival rate. Chaudhary et al. [76] leverage the benefits of BC technologies for the transportation network

and use SDN to provide low power consumption and legitimate resources. Secure and reliable energy management is also considered in [77] where the authors design a cyber-secure decentralized framework to ensure reliability, efficiency, and sustainability jointly using SDN and BC.

With a specific focus on fog environments, Muthanna et al. [69] introduce an IoT-based fog system that incorporates BC and SDN. In detail, SDN can attain high privacy, availability, and security for IoT-based applications, while BC assures decentralization in a secure way. Furthermore, they investigate latency, network efficiency, and resource utilization for the experimental evaluation of their architecture. Similarly, Sharma et al. [73] present a novel BC-based distributed cloud architecture with fog nodes acting as SDN controller at the edge of the network, thus proposing an innovative combination of fog computing, SDN, and BC, along with an architecture for supporting availability, real-time data bringing, scalability, security, resilience, and low latency. Using this architecture, they also evaluate throughput, response time, and accuracy in detecting real-time attacks.

IoT networks are considered in [71], where authors present a model for facing present IoT challenges with SDN and BC in the context of 5G networks. They also introduce the elliptic curve digital signature algorithm for security purposes which is evaluated in a simulation environment. The challenges for securing cloud management from network perspective are investigated in [78], whose authors take advantage of SDN and BC to perform secure cloud management. An infrastructure incorporating both these technologies is developed to improve the availability of cloud systems through the automatic provisioning of network bandwidth. Derhab et al. [72] also face security challenges in an IoT-based industrial environment via a control framework leveraging BC–SDN integration. Moreover, Open-Flow based flow rules are installed in this industrial IoT network effectively exploiting the SDN paradigm. The presented SD-WAN model admits two additional elements, namely: (i) an IDS which can defend against attacks using the joint combination of random subspace learning and K-nearest neighbors methods (*RSL–KNN*), and (ii) a BC-based integrity checking system.

Differently, Qiu et al. [79] deal with the consensus problem in BC for software defined industrial IoT. To address such a problem, the authors use a Q-learning approach showing also its effectiveness via simulations. Shao et al. [80] also present a consensus algorithm named *simplified practical Byzantine fault tolerance (SPBFT)* to transmit messages in the SDN network securely. Specifically, the authors apply this BC approach in an SDN environment to create a readable, addable, and unmodifiable decentralized database. Also, to enhance the security and reach consensus in the SDN control layer, they leverage the proposed SPBFT algorithm to transfer messages between controllers. Finally, they compare SPBFT with the practical Byzantine fault tolerance algorithm proving that the proposed algorithm can significantly improve performance in terms of security and efficiency. On the same line, Liu et al. [81] define the *TrustBlock* method to calculate the trust value of SDN network node based on BC. More in detail, the authors leverage SDN to assess the legitimacy of the nodes and BC to ensure the trust value authenticity, immutability, and openness. The weight of each evaluation attribute is determined using an entropy-based method. BC is also considered as a solution to improve the SDN security of

IoT-based applications interacting via inter-cloud communication in [82]. Basnet and Shakya [83] propose *Blockchain security over SDN (BSS)* to protect the privacy and availability of resources against non-trusting members. The authors demonstrate that BSS facilitates files sharing among SDN users in distributed P2P basis using OpenStack as a cloud storage platform. Additionally, Kataoka et al. [84], propose a Trust List that represents the distribution of trust among IoT-related stakeholders and aims to verifying and trusting IoT services and devices avoiding undesirable traffic of IoT devices responsible for attacks on the network system. Firstly, they verify that IoT traffic management is properly achieved using their proposal. Then, they discuss and implement a proper combination of BC and SDN to ensure security, dependability, and trusting for IoT services and devices. Finally, the proof of concept open-source implementation is tested on both public and private BCs.

Steichen et al. [85] propose *ChainGuard*, which utilizes an SDN module to manage network collisions and implements a firewall based on BC. Furthermore, ChainGuard can offer access control capabilities and can effectively mitigate flooding attacks. Finally, the authors discuss other aspects of the proposed architecture and provide observations on their experiments with the aforementioned model. Similarly, Abou El Houda et al. [86] present framework sharing SDN and BC to mitigate DDoS attacks in a scalable, stable, and cost-effective manner. Another possible application is proposed in [87] whose authors introduce a consolidated BC–SDN system that manages spectrum assets to enable interoperability between mobile network operators over small cells.

## 4 Security and Privacy Issues in BC–SDN Systems

This section covers security and privacy issues concerning BC and SDN technologies and their integration. Precisely, in Sect. 4.1, we discuss issues in BC, also addressing those related to scalability and confidentiality. Section 4.2 deals with security management in SDN with particular focus on IDS. Section 4.3 describes issues arising when integrating BC with SDN and also reports new challenges faced in this context.

### 4.1 Security and Privacy Issues in Blockchain

As described in Sect. 2.1, BC is widely used in different domains that take advantage of its unique properties. Nevertheless, dangerous attacks can cause several issues in BC-based networks. In the following, we describe some security issues that attackers exploit to undermine the safety and cause damage in BC systems [88].

#### 4.1.1 Majority Attacks (51% Attack)

When BC uses PoW to reach consensus, the probability of mining blocks depends on work done by miners. If a miner holds 51% (i.e. more than half) of total computing power, it can monopolize the mining process and take control over the

BC to decide which block is validated and then added to chain [88]. Based on this reasons, miners could join together to mine more blocks, thus constituting a "mining pool", that is a group of nodes holding most of computing power. In such a situation, miners (organized in a mining pool) can modify the transaction data (potentially causing double-spending attacks), alter their order, and stop the mining of other available blocks [89].

#### 4.1.2 Forking Attacks

In a BC system, users can propose changes of BC protocol or software. When this situation occurs, miners have to decide which version to use and if there is not a unanimous decision, two BC versions are created. Therefore, nodes can be divided into two types: old and new nodes.

Forks are categorized into two types: *hard-fork* and *soft-fork*.

- *Hard fork:* a hard-fork is a significant change within a cryptocurrency protocol that is incompatible with the previous version. It usually changes or improves an existing protocol or creates a new independent protocol (and consequently a new chain). The node that does not update to the new version will not be able to process transactions or push new blocks to the BC. If a group of nodes continues to use the old version, a permanent split occurs in the BC.
- *Soft fork:* a soft-fork is actually a change in a cryptocurrency protocol that is back-compatible and where non-updated nodes are able to process transactions and add new blocks to the BC.

With forking attacks, malicious users can replace the longest chain (also referred to as the most trusted chain) on the current network with another chain to gain personal benefits. Therefore, reducing the generation of fork to the minimum necessary is the most directly method to defend against forking attacks in a BC system.

#### 4.1.3 Selfish Mining

Selfish mining constitutes another significant concern for BCs. During this attack, the malicious miner maintains the mined blocks without broadcasting them towards the networking system and generates a personal chain where he is the only one producing blocks that are revealed only after particular requirements (chosen by the attacker) are fulfilled. In other words, the attacker generates a secret longer chain that when revealed would have more "chain-work" (viz. PoW) than the public shorter chain, and thus will be followed by other miners cancelling the revenues obtained on the public chain in the meantime. Therefore, in this case, reliable miners spend lots of time and resources without obtaining any revenue, while selfish miners continue to mine their individual chains obtaining high revenue after revealing them [52].

#### 4.1.4 Social Engineering

Social Engineering is an attack conducted by outsiders using psychological tricks to get users' personal information to access a computer or even a whole network [90]. Social Engineering is a main issue afflicting BC security: according to [91], in 2018 almost $3 billion was lost due to social engineering. To perform this attack, phishing is one of the most used technique. The attacker sends the targeted users a fake URL or website links on the behalf of a company or organization brand he trusts. Commonly, they pretend that his account has some security issues and ask the users to send their information through provided links to solve such issues, claiming that otherwise his account will be blocked. The ultimate aim of the attacker is to put pressure on the user and hands over his information. Social engineering attacks are particularly target toward crypto users and realized via phishing among which SIM swapping is one of the most utilized.

#### 4.1.5 Privacy in Blockchain: Confidentiality and Authentication

A BC is a decentralized and distributed technology composed of a huge number of interconnected blocks which contain key information generated by different parties mainly for business purposes [92]. Researchers are attracted by the properties of BC and have proposed it for IoT, Industry 4.0, and many other environments to increase security and privacy.

As described, BC uses consensus mechanisms such as PoS and PoW being independent of any third party: confidentiality and secrecy of transactions are guaranteed since they are not verified and owned by a single entity. Another technique named *Zero-Knowledge Proof* transmits the information to an examiner to identify whether the transaction is valid or not [93]. The goal of such a technique is to hide the internals of a transaction revealing just its validity and thus guaranteeing the full confidentiality of the transaction details.

Moreover, to preserve the privacy (i.e. to further guarantee their confidentiality), the transactions are secured via *public-key cryptography*, and once a block of information is included in the chain, it cannot be altered or modified [94]. Public-key cryptography is also exploited for digital signature used for transaction authentication in an untrustworthy environment [31]. In detail, the BC leverages public-key cryptography to send transactions and verify their authentication. The transaction is signed using the sender's private key, before being sent over the P2P network (see Fig. 7). To this aim, existing BC typically employs the elliptic curve digital signature algorithm. As shown in Fig. 7, P2P networks with the aid of global ledger give users the complete control on their data to ensure confidentiality and authentication to different applications, decreasing the threat of third parties to sell, store, or manipulate personal information. Typical applications needing such privacy requirements are financial transactions, healthcare record, and legal documents (cf. Sect. 5).

Furthermore, BC is capable of providing privacy by storing data transactions as blocks with hash values. The blocks are organized as a mesh like structure and are encrypted and decrypted via public and private keys, respectively [95]. During this process users exploit the hash value of the public key as their address and can also

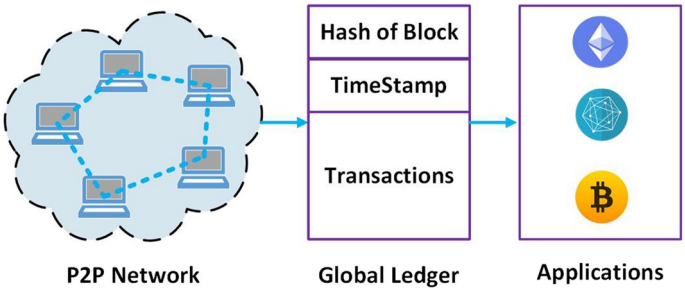



**Fig. 7** Overview of confidentiality and authentication process of a Blockchain

generate several addresses. This in turn keeps the real identity of a user. In such a way, data confidentiality is preserved, and each transaction can be checked with the aid of the consensus process and the logs inside the BC. Indeed, using this procedure, every transaction is rechecked until it is globally included: it is first signed by the recipient and then added with a digital signature. Overall, all these procedures help to guarantee the integrity of data transferred within the network and maintain the most sensitive data confidential [96].

### 4.1.6 Authorization

When data reside in and are managed by a single organization, dealing with security and privacy issues is relatively simple. Conversely, when the information is exchanged between different domains—as when leveraging BC—securing data is a much more complex process. Secure access control mechanism is a common approach used to ensure that only authorized entities can access shared data. Such a mechanism involves access policies commonly consisting of access control lists (ACLs) associated with the data owner. An ACL is a list of requestors who can access data, and provides related permissions (i.e. read, write, update, delete) to specific data. Hence, the authorization is a function of granting permission to authenticated users to access the protected resources following predefined access rules. Access rules mainly focus on who is performing which action on what data object and for which purposes.

Commonly, traditional authorization approaches are deployed, managed, and run by third parties (e.g., cloud service providers) that can be benign but curious. To build a trustworthy system, the BC can be combined with an access control mechanism, realizing a self-management of users' own data, and thus keeping shared data private. For instance, BC users can leverage SCs (cf. Sect. 5) to define access permissions (i.e. authorize, refuse, revoke), operations (i.e. read, write, update, delete), and duration of their data sharing without the loss of control right. SCs can be triggered on the BC once all the preconditions are met and can provide an audit mechanism for any request recorded in the ledger as well. A notable application of BC-based authorization leveraging SCs is for securing healthcare data sharing [97].

#### 4.1.7 Other Issues

Given the rising number of transactions, the BC volume grows on a daily basis, and scalability issues have to be taken into account. Indeed, every single node must save every transaction to verify all of them when needed. For instance, Bitcoin—the most common crypto-currency using BC—has to process $\approx 7$ transactions per second [98]. Given the small size of a block capacity, Bitcoin can not handle or process the millions of transactions in real-time, and many small transactions are delayed. Consequently, miners request high fees to process and validate them.

Additionally, confirmation time is another challenge to consider when operating with decentralized P2P transactions as in BCs. More specifically, each transaction takes an average time between 20 and 40 min for confirmation [99]. Optimization strategies based on division of BC nodes, taking into account the number of computers the user has to access the network, have been proposed to reduce confirmation time up to more than 70% [100].

### 4.2 Security Management in SDN

As shown in Sect. 2.2, SDN is a scalable networking paradigm consisting of three planes: the application, control, and data plane. To secure SDN and lead to adequate protection, the first step is to understand the weaknesses of each of them. Indeed, it is worth noticing that the security of the overall system can be achieved by securing all the above-mentioned planes. However, because such planes are separated [92], the protection of the whole system needs also to be assured. In this sense, to secure the SDN model from attacks and intrusions, an additional plane can be added: it comprises attack and IDSs, and a firewall to defend the network and guarantee its availability [101].

Generally, in an SDN, users access data from various controllers, thus implementing a new architecture where they ask permission from the controller may protect the system from malware. On the other hand, networking devices (e.g., switches, routers, storage systems, and sensors) are involved in packet forwarding and located in the data plane. In addition, specific tools, such as *Flow Checker*, *VeriFlow*, and *FortNOX* can be used to effectively manage the packets by systematically forwarding or deleting packets thus increasing network efficiency [58]. OpenFlow can assist devices in determining the exact match of the packets [102]. While attack detection protects the network from the intruders, data encryption handles users authentication and protects the data from being manipulated by the attackers. In addition, the state of the network can be determined by analyzing the information processed by the control plane. In the last years, different tools have been proposed to support network administrators like *Athena* [103] that performs anomaly detection via a scalable approach.

As depicted in Fig. 5, in an SDN environment, there can be multiple controllers (communicating via the eastbound/westbound API) or a single centralized controller. Data transmission is performed by the switches following a flow table

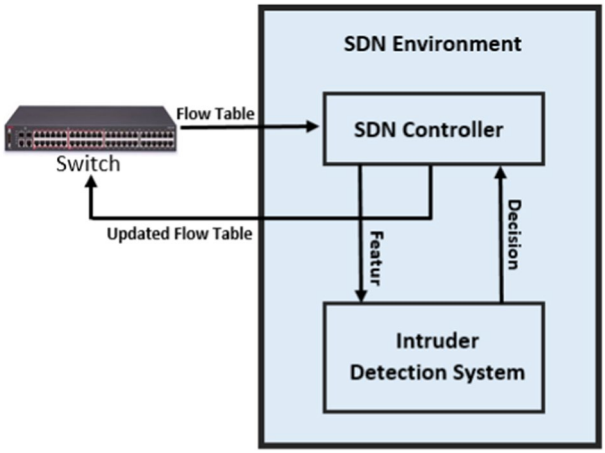



**Fig. 8** Block diagram of an IDS

that contains information about the connections and their properties [104]. These devices take specific decisions for each request coming from different connections. In this context, a malicious user can shake up the normal traffic flows in the network. For example, an intruder may send different request for the same service to damage the network or sends a message that corrupts network devices. These are examples of common situations in which an IDS can help to ensure security [105]. Figure 8 depicts the main components of an IDS with the principal information exchanged among its blocks when applied in an SDN. Based on the information exchanged with the controller(s), the IDS can guide the update of the flow table to avoid malicious threats conducted by an attacker. To attain this goal, some researchers propose to check for the entropy of the IP addresses to discover anomalies regarding the users, and then analyze the flow table to figure out some useful features to build machine learning (ML) models for future predictions on unseen data [106, 107].

### 4.3 Security and Privacy Issues of BC–SDN

The combination of BC and SDN helps to improve the efficiency of smart architectures such as: smart grid, education, healthcare, industry, transportation, etc. Nevertheless, security continues to be a severe concern for these systems, and efforts are needed to solve challenges and issues as described in the following.

#### 4.3.1 Aim and Challenges of BC–SDN for Security

The SDN-based system separates the control plane from the data plane to provide more flexibility to the network. However, the control plane is the main target of the intruders who can easily take control over it. Therefore, BC–SDN aims to improve the overall security and flexibility of the networking system [80]. BC is compatible with both private and public environments and it can be useful for

securing P2P communications. For transferring file securely in IoT networks, BC provides security, while SDN is also beneficial for reducing energy consumption [108]. For these reasons, we can identify many areas where there is a need to implement the integration of SDN with BC.

However, several challenges concerning this combination still remain, and the systems where the joint combination of the two techniques is applied have to deal with some issues. Firstly, the planes of SDN networks can be accessible from the intruders who can obtain information such as host IP or the networking architecture performing simple scanning operations [109]. Leveraging these data attackers can manipulate packets and launch several attacks such as *ARP* or *IP spoofing* [110]. Moreover, if a host network is attacked then the intruder can easily take control and manipulate the communication from the control plane carrying out a *hijacking* attack [111]. A *man in the middle* attack instead aims to take control over the SDN flow tables and rewrite their content.

BC has been proposed as a viable way to protect the SDN environment but actually it is not a silver bullet for all SDN security concerns and some challenges remain open. Among possible attacks, DDoS is one of the most dangerous one [112] since it impairs the availability of the chain and can allow attackers access to associated wallets and exchanges. Also, the presence of unauthorized users might create security issues such as malicious access to wallet and refuse to allow new blocks from entering the BC. Moreover, in the BC-based system, transactions data are usually store on public chain so that anyone can easily get access to the records. This would create important issues for environment where transactions are meant to be secret (e.g., bank transactions). Time and cost are another two challenges of integrating BC with SDN. Since smart systems need to deal with several quick-access tasks, the lesser the time, the higher the efficiency.

#### 4.3.2 Confidentiality and Privacy in BC–SDN

Along with security, privacy is a key concern also when considering the integration of BC with SDN. Indeed, the combination of such technologies can significantly help in reaching this goal. As discussed in Sect. 4.1, BC stores information in the blocks after performing cryptography and data hashing, thus privacy is guaranteed, and personal information could remain confidential. Since centralized systems can be affected by single point of failure [113], decentralized structure of BC comes up to reduce this vulnerabilities [94]. In SDN, data privacy could be undermined by the collection of the information since raw data are gathered from different types of device and processing procedures can corrupt data integrity. Considering a real use case, the deployment of closed circuit television cameras for security purposes is becoming extremely common in smart environments, and as a result, people can barely attain a complete privacy because they feel monitored all the time with consequent discomfort. BC could be applied for privacy protection so that actual records are shown only to authorized users; otherwise the videos are blurred by the system [114].

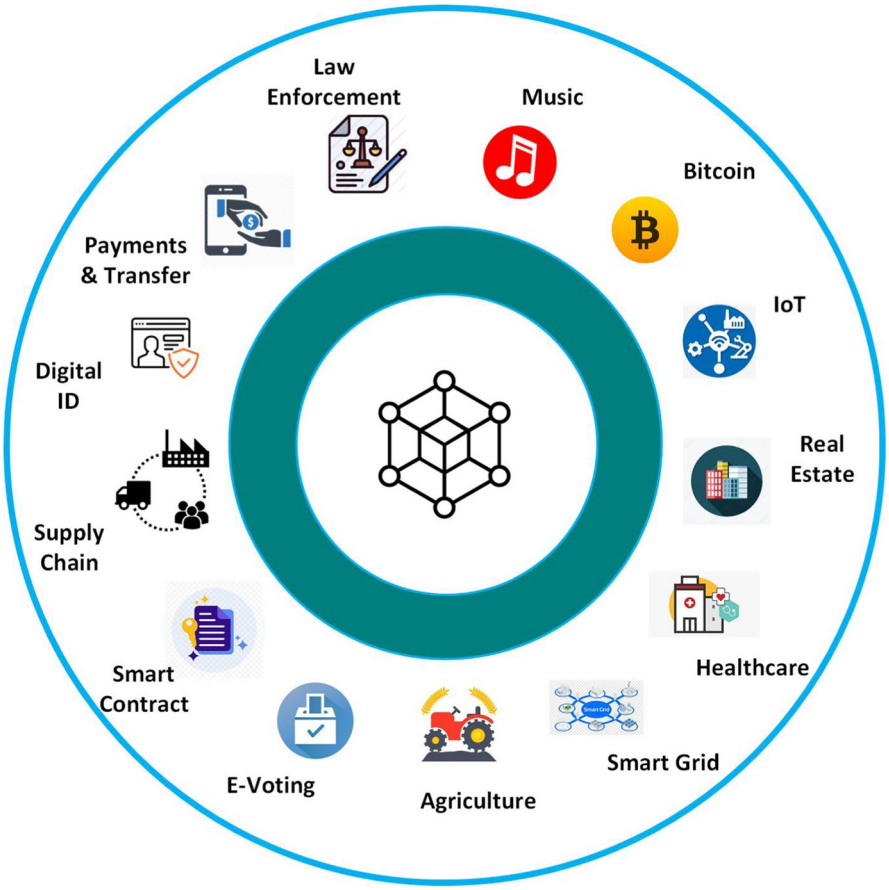



**Fig. 9** Blockchain applications

## 5 Notable Applications

This section describes applications developed thanks to facilities and properties offered by studied technologies. Section 5.1 provides the description of the most important apps supported by BC technology; the last section discusses the ones built by integrating SDN with BC (Sect. 5.2).

### 5.1 Blockchain Applications

BC technologies are used in many areas, not only in financial applications. Figure 9 collects some of the application fields of BC technology covering several industrial sectors. In the following, we describe some of the most common BC applications. For the sake of completeness, other interesting ones are reported in Table 3 where

**Table 3** State-of-the-art works focusing on the utilization of Blockchain in different application fields

| Reference | Year | Application field |
|---|---|---|
| [115] | 2021 | Application of BC for the sustainability of Prefabricated Housing Construction |
| [116] | 2021 | Barriers for adopting BC technology in sustainable supply chains |
| [117] | 2021 | Constructing a smart city IoT framework with BC and SDN that is energy aware and distributed securely |
| [118] | 2021 | Blockchain application for supply chain in the area of construction industry |
| [119] | 2021 | Blokchain technology for the safety of the management of food data |
| [120] | 2021 | Application of Blockchain for financial sector |
| [121] | 2021 | BC-based architecture for intelligent vaccine distribution approaches in COVID-19 pandemic situation |
| [122] | 2021 | Integration of Blockchain for Supply chain management |
| [123] | 2021 | Blockchain-based privacy for smart healthcare management |
| [124] | 2020 | Impact of BC on applications covering different industrial sectors |
| [125] | 2020 | Effects of BC technology on the logistics industry and other business models |
| [126] | 2020 | Framework for the analysis of BC integrating institutional, market, and technical factors |
| [127] | 2020 | BC-based decentralized app for smart building system management |
| [128] | 2020 | Blockchain-based security for cloud storage management in IoT networks |
| [129] | 2019 | Applications in the architecture, engineering, and construction industries |
| [130] | 2019 | BC-enabled SCs in different application scenarios (e.g., finance, energy, etc.) |
| [131] | 2019 | Review of the BC systems exploited in the oil and gas industry |
| [132] | 2019 | Main trends of BC usage in supply chains management and logistics |
| [133] | 2019 | SDN–IoT model with NFV implementation for smart cities based on a distributed protected BC architecture |
| [134] | 2019 | Applications for smart communities (e.g., smart grid, transportation, healthcare) |
| [135] | 2018 | BC-connected gateways to maintain user privacy in IoT networks |
| [136] | 2018 | `LedgerGuard`: a tool for ledger integrity, detecting and recovering corrupted blocks |
| [137] | 2018 | Patient monitoring system using SC and private BC based on the Ethereum protocol |

**Table 3** (continued)

| Reference | Year | Application field |
|---|---|---|
| [138] | 2018 | Potential applications of BC in travel industry |
| [139] | 2018 | Decentralized apps and design of a certificate system based on Ethereum BC |
| [140] | 2018 | Model for academic certificate verification using BC technology |
| [141] | 2018 | *BC for Education* to support protection and secure management of certificates |
| [142] | 2017 | Lightweight instance of a BC system for smart home environments |
| [143] | 2017 | Current and possible future applications of BC in various domains |
| [144] | 2017 | *FruitChains*: a new protocol to ensure fairness in a BC |
| [145] | 2016 | BC-based distributed system for educational record and reputation |

The works are reported in reverse chronological order

recent works are summarized along with their application fields and related contributions. Unfortunately, almost all of such systems providing smart services (and their actual applicability) are validated and evaluated in simulation environments given the high cost needed to employ them in production.

*Bitcoin and Cryptocurrencies.* Bitcoin is a cryptocurrency, often described as digital or virtual currency because when using it, there are no bank transactions or any physical medium. Mining is a process originated from bitcoin systems where miners verify transactions and can earn bitcoin when validating a particular number of transactions. Bitcoin is stored in wallets which are referred to as a string of letters and numbers. These can be a piece of paper, a hardware device, or online-based. A physical bitcoin is useless if it doesn't have any private codes inside. Starting in 2009, the cryptocurrency unit price was only 0.01; nowadays 1 bitcoin is worth $\approx 40k$. Notably, the value of bitcoin has price ups and downs when exchanged with traditional currency due to politics, media hype, and country acknowledgements. Without being exhaustive, other than bitcoin, the most important BC-based cryptocurrencies (based on their market cap) are Ethereum, Litecoin, Tether, Binance Coin, and Cardano.

*Supply Chain Management.* We now discuss complex supply chains that extend to all parts of the world [146]. All physical products should take a journey from the seller to the buyer, and the process that allows to transfer such products is referred to as supply chain. In this context, transparency is related to the information accessible to firms composing the provider network [147]. The path to the consumer is not straightforward and sometimes there are dozens of intermediaries involved. The BC technology can potentially improve the transparency and traceability within the manufacturing supply chain through the use of the immutable record of data, distributed storage, and controlled user access [146].

*Healthcare.* Nowadays, the use of IoT in medical care is rapidly increasing because of the impressive growth of medical data. Sharing such data is a critical aspect for improving the quality of healthcare services and reducing medical costs. The concept of protected healthcare information has been introduced to handle secure and trusted data transactions for transmitting and storing medical data. Indeed, though current healthcare systems bring much convenience, many obstacles still exist in practice, that hinder secure and scalable data sharing across multiple organizations, and thus limiting the development of medical decision-making and research. Particularly, in a centralized system, there exist risks related to the single-point of attack and data leakage. This may result in unauthorized use of patients' private data by curious organizations. In this case, it is necessary to ensure security and privacy-protection and return the control right of data back to users to encourage data sharing.

BC-based SCs are introduced to facilitate secure analysis and management of medical sensors and to ensure data security and authorization (cf. Sect. 4.1) for patients and medical professionals [97, 137]. Figure 10 depicts a healthcare transaction using the BC and the different stakeholders involved, showing how BC-based systems establish a secured connection between the doctor, patient, and data analyst in healthcare organizations to manage the patient records securely. In such a way, the BC can address a variety of problems (e.g., care coordination, health data security,

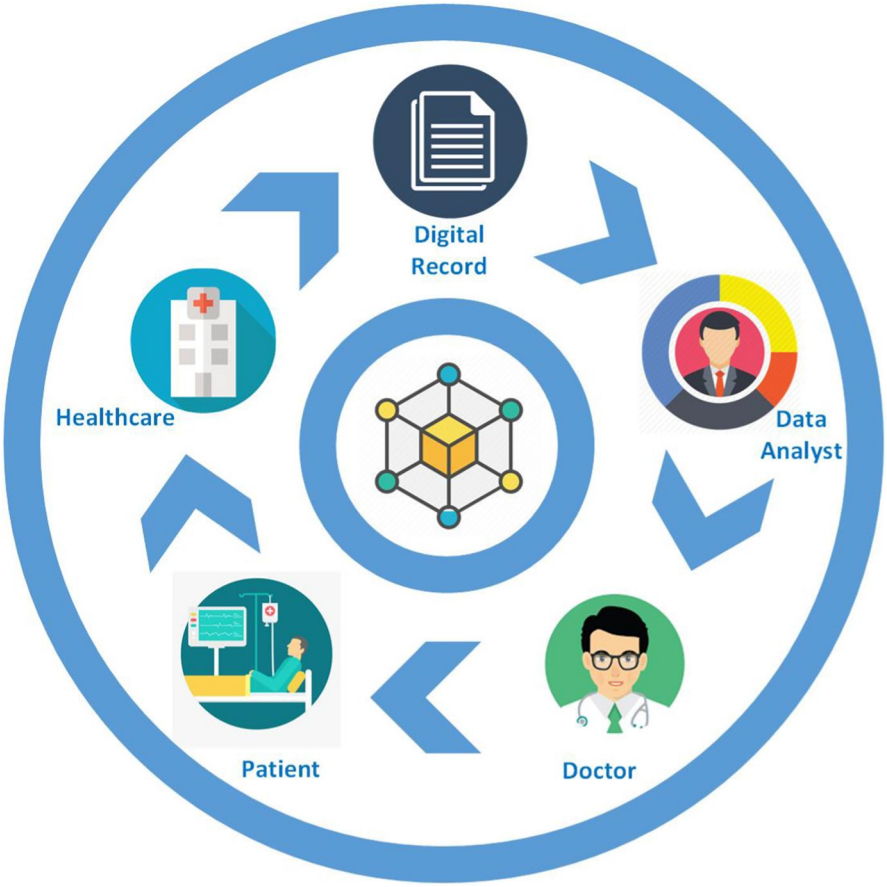



**Fig. 10** Exemplifying healthcare transaction using Blockchain

and interoperability issues) since—as shown in Fig. 10—it can harness the data stream to improve the quality of care by sharing medical records, protecting sensitive data from threat actors, and giving patients more control over their information. The BC can aggregate a patient's medical and prescription records from multiple sites/providers to generate a single, up-to-date aggregate record that medical professionals can comprehensively refer to when treating patients.

*E-voting.* E-voting is an election voting system where users cast votes through a digital system with a secure, reliable, and secret balloting over the Internet. Many countries in the world use the e-voting system for its anonymity security, reliability, integrity, and availability. The BC with the SCs emerges as a good candidate to develop a cheaper, more secure, more transparent, and easier-to-use e-voting system [148]. Using BC, the main focus is to make the voting process fair and without any third-party mediation. There are many platforms to deal with the e-voting systems; one of them, Ethereum, is a widespread network for deploying such applications.

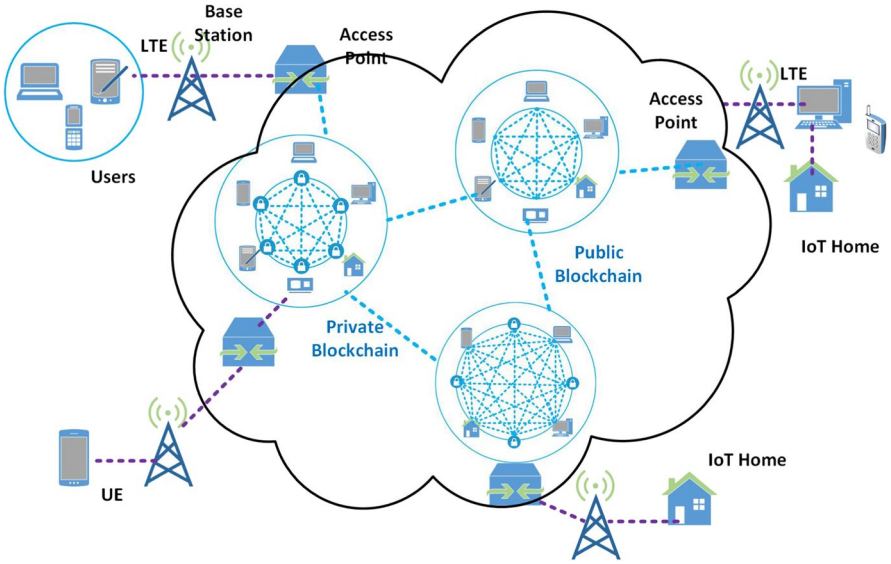



**Fig. 11** Integration of the Blockchain in an IoT environment

The main concern in this scenario is to protect the users' identity and preserve transparency and integrity of data. To face this challenge Ethereum provides different hash values to users in the network through which it is almost impossible to identify the individuals. At the same time, each transaction is visible to everyone in the network [149] and can be validated: this makes it transparent to all the nodes in the network and maintains the integrity of data. Moreover, in distributed databases, data are stored in particular locations, making the data unmodifiable and thus the vote can not be manipulated.

*Smart Contract.* An SC is a protocol that digitally facilitates the verification, control, or execution of an agreement. It is a compromise between two or more parties in the form of a digital code. On the BC, participants run these codes which are kept in a public database and are unchangeable. In other words, SCs are a set of rules, and the BC manages the transactions that meet them so that they can be delivered automatically without a third-party. With a contract, some conditions needs to meet up; in this case, both rules and data are stored in the BC. Moreover, if any illegal transaction according to the SC occurs, the BC can swiftly rollback the transaction [66]. Summarizing, SC is acknowledged as a contract having as features self-execution, transparency, flexibility, and self-enforcing [150].

*Internet of Things.* IoT presents a massive variety of devices offering possibilities for remote monitoring in numerous applications of several domains [151, 152]. IoT is widely used in smart industries, smart transportation, healthcare, military/battlefield-things, etc., and it is considered a revolution which is changing our world. Given its impressive dimensions and distributed nature, privacy and security are the main concerns [153, 154]. Many frameworks are proposed to secure IoT environments; among them BC is increasingly used to make IoT platforms secure [155]. In

BC-based IoT systems, as shown in Fig. 11, private BC performs tasks efficiently and at low cost in closed environments, whereas public BC can establish connections between multiple IoT environments once at a time. In this case, management of trust is crucial and is maintained centrally without any third-party involvement.

*Hyperledger.* Hyperledger is an open-source collaborative effort that has been established to advance BC technologies. It is hosted by the Linux Foundation, and it is an all-embracing co-operation platform that supports ledgers in supply chains, banking, manufacturing, IoT, finance, and technology. In simple terms, Hyperledger can be thought of as a software that enables developers all across the globe to develop BC-based solutions for particular businesses [156].

*Industry 4.0.* Recently, industrial activities are advancing towards automation [2]. Activities that do not strictly require human intervention are performed with the help of several automated technologies, and BC is one of the most important. With its properties and the help of encrypted algorithms, nowadays it has been applied (or proposed to apply) to different industrial sectors [157, 158]. For instance, in the power electronics sector, through this technology, a producer can submit an offer for a certain device, while engineers evaluate and decide whether to accept it. In case of no matching, the producer has the possibility to resubmit the offer to reduce the mismatch with the supply [159]. Flexibility, authorization mechanisms, and protection must be guaranteed when moving to the automation process. BC allows a more sustainable and scalable ecosystem for smooth industrial operations supporting other innovative technologies such as edge computing [160]. Moreover, Industry 4.0 depends on data received from multiple sources which are processed to produce an outcome. The entire framework would fail if data are not properly validated. Also, ensuring their protection is necessary so that a third-party can not compromise the data. In this respect, BC can provide Industry 4.0 framework with unalterable, secure, and privacy-preserving data storage [161].

*Others Applications.* Apart from the above-discussed applications, BC is also used in finance, business, government, asset management, insurance, personal identification, real estate, and many other fields as summarized in Fig. 9.

### 5.2 BC–SDN Applications

The integration of BC and SDN can offer various systems some remarkable features. For example, in [87], the authors introduce a particular deployment approach for *multi-operator small cells* exploiting the fusion of BC and SDN. In detail, BC is implemented above the SDN platform that qualifies the operations within the network. These two technologies are also used in *vehicular networks*, especially for security purposes because SDN provides flexibility and BC offers trust to the network.

Generally, to diminish the vulnerability of the huge number of network devices, SDN control plane is not satisfactory: this is why BC takes the place to *validate insertions into flow tables* [8]. Researchers propose to send the information from network devices via BC agents which act as the mediator plane to verify insertions

and are enforced between the SDN switches and SDN controller. This mechanism is responsible for vicious flows.

The monocentric architecture of SDN exposes it to a great range of attacks; for this reason, private BC is used to manage the resources along with the other technologies [162]. In some particular contexts, SDN controllers are used to make a *chain of controllers* as if each of them constitutes a block of the private BC. Encryption is also used before storing the information and also to establish *P2P connections* between SDN controllers and other devices [163].

A private BC is used in each domain of an SDN, while each SDN controller is associated with other controllers through a public BC. In this way, security of SDN is attained, while a significant number of works aims to improve the performance of cloud storage combined with BC–SDN. For instance, in [73] a *distributed BC cloud architecture* based on software-defined fog nodes is presented. In the *fog layer*, the SDN controllers realize a distributed network forming a BC, while in the cloud layer, another BC is constituted with the *cloud storage*. When *multiple controllers* are deployed in an SDN, BC can also harmonize their joint cooperation.

There are many other examples where these two technologies are employed in concert [164]. Indeed, although SDN has extremely valuable benefits, it requires BC support especially into the control plane to guarantee the security [80]. For example, to mitigate DDoS attacks, in [68, 165] is investigated the usage of *SCs in the Ethereum platform*, whose rules are programmatically defined in the SCs.

## 6 Challenges and Integration with Emerging Technologies

In this section, we firstly discuss limitations and challenges of BC–SDN integration, then we present some emerging technologies that can be used along with the ones we have analyzed in this survey to offer valuable facilities for new applications.

*Limitations and Challenges.* Possible limitations of BC–SDN integration are specifically related to the real-world implementations of solutions based on it. In fact, most of the previous works have demonstrated its functioning and benefits in a simulated environment, without evaluating its actual feasibility. When assessing real-world implementations, the scalability of the state-of-art solutions is an open issue. For instance, if BC–SDN is exploited for managing and securing a considerable number of nodes in an IoT scenario, it may incur severe performance degradation or even failures. Also, the performance of an actual system could be severely impacted by the specific BC implementation leveraged since the most convenient platforms come at a huge cost in terms of implementation, processing, and energy: this is still an open challenge in both the research community and industry (e.g., finance and technology sectors).

Another open challenge of SDN is related to synchronization. More specifically, there is a lack of standardized methods to support synchronization in SDN. Additionally, data confidentiality in BC should be carefully managed by taking into account the public visibility of BC among its users [33]. This could cause distrust in governments and organizations in widely employing such technologies when managing and sharing sensible data.

*Blockchain for Big Data Analysis.* Data science is becoming the heart of today's world. It is a fact that individuals and corporations with huge amount of data, information, and knowledge extracted from them would have a great advantage in modern business and government. The techniques to analyze and deal with the high dimensional data are another key topic in modern research and are commonly known as Big Data analysis. Since BC immutably stores records of information through blocks, it will provide newer services and technologies for such analyses. Indeed, data transactions will be more secure if BC can predict some patterns about the upcoming records. Also, data would be accessible to various interested actors participating in the chain without possible errors or corruption.

*Blockchain for Robotics.* Robotics is another fundamental application field strictly related to artificial intelligence (AI). AI-enabled robotics together with BC could be exploited to implement bots that execute their operations communicating with cloud/fog systems without interrupting their operability because of data corruption or manipulation (due to attacks or not). Indeed, BC could prevent illegal instructions from being injected into the robots, thus securing both authentication and operability. The remote decision making process for robots functioning based on BC would also decrease the complexity in terms of both time and space.

*Advanced Services via Holochain with AI-enabled BC.* A main drawback of BC is that it is characterized by a considerable computation complexity, and it needs more memory with the increasing volume of transactions. Holochain is an alternative technology that could replace BC to ensure privacy and security in IoT networks, and has already gained the attention of researchers [166]. More specifically, Holochain moves from the data-centric structure typical of BC to an agent-centric one. Indeed, Holochain blocks are independent and each possesses its "hashchain", without the need of reaching the consensus for data validation. Such a distributed architecture can significantly improve scalability via the proper integration of microservices and distributed application with always-online devices (e.g., IoT sensors) [167]. If, on the one hand, Holochain can better manage the scalability problem experimented by BC due to the increase of the transactions volume, on the other hand, BC could be used in combination with Holochain to offer different services that can take advantage from both technologies. For instance, Holochain can be used to develop different distributed BC solutions that can communicate to each other. Additionally, combining AI into such a system can improve the security control in Holochain when needed. Moreover, BC can continue to be exploited for transaction storing and authentication in smaller networks.

*Machine and Deep Learning with Blockchain.* Commonly, BC adds a new block of transactions to the chain after reaching the consensus (e.g., based on PoW) and performing the authentication of every single transaction. Authentication task can be automated using SCs that are blocks of predefined instructions allowing trusted transactions amongst the anonymous nodes without the presence of a central legal authority. This process leveraging SCs could be replaced by ML approaches that would exploit a dynamic trained model rather than a fixed set of predefined rules. Deep learning (DL) is slightly different from the traditional ML paradigm. Indeed, DL models are trained directly from input data and can attain higher accuracy especially when working with unseen data (e.g., via unsupervised or semi-supervised

approaches) [168]. As seen in previous sections, IoT sensors generate huge amount of new data in real-time, while BC is successfully exploited for secure transactions. In these systems, DL models can be deployed to perform automatic operations enhancing the performance of ML approaches and efficiently providing several automated online services. Overall, by using DL to manage the chain, security can be also significantly enhanced [169]. Moreover, since such models work better with large amount of data, they can take advantage of the decentralized nature of BC fostering data sharing.

## 7 Conclusion

In this survey, we have investigated two different technologies which have found extensive application in network-related scenarios, namely BC and SDN. Firstly, we have provided a thorough overview of each technology discussing also their main features, opportunities, and facilities they can provide to modern applications. Moreover, we have explored the innovative integration of these technologies—named BC–SDN—proposed to face challenges of modern networking scenarios. Indeed, BC–SDN allows security, reliability, flexibility, cost-effective management to different applications in various networking fields. In this regard, we have reviewed and discussed state-of-art proposals providing both motivations and details. Security and privacy issues are one of the most important factor driving the integration of innovative technologies, thus they have been a key focus of our discussion. We have then analyzed such issues related to considered technologies and their integration. Actual applications of BC, SDN, and their integration are further described to provide a real-world flavor to our discussion, showing that current "smart" application fields can not disregard the fruitful utilization of such technologies. Finally, the integration with further present and emerging technologies (e.g., Robotics, AI, Holochain) is also envisioned and discussed.

It is worth noticing that the integration of BC with SDN can help to shape their social impact. The improved manageability, transparency, and security of applications exploiting BC–SDN would rebuild the bridges between centralized systems and application users thanks to its tracked, audited, and (if needed) publicly accessible data. Indeed, such peculiar features offer far-reaching possibilities for social impact, such as transaction transparency, personal data protection, legitimacy, compliance, trust, etc. As discussed previously, the potential use cases span from financial transactions to e-voting and healthcare in which (monetary/election/medical) data can be safely stored and are instantly available to stakeholders when needed, also in case of emergency. However, if, on the one hand, there are a lot of opportunities and advantages, on the other hand, it is hard to forecast if such a shift will happen. Indeed, this depends on how organizations and governments will embrace such technologies: depending on its deployment, a given technology can either be disruptive or transformative.

In view of the outcomes of the present survey, we think that the fruitful trend of jointly using BC and SDN will continue and produce positive synergy. Several domains and applications would benefit from such an integration, and both

researchers and practitioners working in such domains should continue exploring BC–SDN integration with the aim of providing advantages such as management flexibility, scalability and data flow verification. In fact, there is room for further research effort for the improvement of security and performance of BC–SDN also in view of upcoming use cases and (sadly) possible threats.

Future avenues that should be investigated are the technical challenges underlining the considered technologies when applied in scenarios having particular constraints in terms of scalability and computational efficiency.

**Funding** Open access funding provided by Università degli Studi di Napoli Federico II within the CRUI-CARE Agreement.



## References

1. Mostarda, L., Navarra, A., Nobili, F.: Fast file transfers from IoT devices by using multiple interfaces. Sensors **21**(1), 36 (2021)
2. Aceto, G., Persico, V., Pescapé, A.: Industry 4.0 and health: Internet of Things, Big Data, and cloud computing for Healthcare 4.0. J. Ind. Inf. Integr. **18**, 100129 (2020)
3. Talari, S., Shafie-Khah, M., Siano, P., Loia, V., Tommasetti, A., Catalão, J.P.: A review of smart cities based on the Internet of Things concept. Energies **10**(4), 421 (2017)
4. Vandana, C.: Security improvement in IoT based on software defined networking (SDN). Int. J. Sci. Eng. Technol. Res. **5**(1), 2327–4662 (2016)
5. Karmakar, K.K., Varadharajan, V., Nepal, S., Tupakula, U.: SDN enabled secure IoT architecture. IEEE Internet Things J. **8**(8), 6549–6564 (2020)
6. Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. Proc. IEEE **103**(1), 14–76 (2014)
7. Al Shuhaimi, F., Jose, M., Singh, A.V.: Software defined network as solution to overcome security challenges in IoT. In: 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 491–496. IEEE (2016)
8. Hu, J., Reed, M., Al-Naday, M., Thomos, N.: Blockchain-aided flow insertion and verification in software defined networks. In: 2020 Global Internet of Things Summit (GIoTS), pp. 1–6. IEEE (2020)
9. Hu, J., Reed, M., Thomos, N., Ai-Naday, M.F., Yang, K.: Securing SDN controlled IoT networks through edge-blockchain. IEEE Internet Things J. **8**(4), 2102–2115 (2020)
10. Mendiboure, L., Chalouf, M.A., Krief, F.: Towards a Blockchain-based SD-IoV for applications authentication and trust management. In: International Conference on Internet of Vehicles, pp. 265–277. Springer (2018)
11. Yurekten, O., Demirci, M.: SDN-based cyber defense: a survey. Future Gener. Comput. Syst. **115**, 126–149 (2021)
12. Ahmad, S., Mir, A.H.: Scalability, consistency, reliability and security in SDN controllers: a survey of diverse SDN controllers. J. Netw. Syst. Manag. **29**(1), 1–59 (2021)

13. Hasneen, J., Sadique, K.M.: A survey on 5G architecture and security scopes in SDN and NFV. In: Applied Information Processing Systems, pp. 447–460. Springer, Singapore (2022)
14. Eliyan, L.F., Di Pietro, R.: DoS and DDoS attacks in software defined networks: a survey of existing solutions and research challenges. Future Gener. Comput. Syst. **122**, 149–171 (2021)
15. Ray, P.P., Kumar, N.: SDN/NFV architectures for edge-cloud oriented IoT: a systematic review. Comput. Commun. **169**, 129–153 (2021)
16. Balasubramanian, V., Aloqaily, M., Reisslein, M.: An SDN architecture for time sensitive industrial IoT. Comput. Netw. **186**, 107739 (2021)
17. Younus, M.U., ul Islam, S., Ali, I., Khan, S., Khan, M.K.: A survey on software defined networking enabled smart buildings: architecture, challenges and use cases. J. Netw. Comput. Appl. **137**, 62–77 (2019)
18. Sahay, R., Meng, W., Jensen, C.D.: The application of software defined networking on securing computer networks: a survey. J. Netw. Comput. Appl. **131**, 89–108 (2019)
19. Farris, I., Taleb, T., Khettab, Y., Song, J.: A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Commun. Surv. Tutor. **21**(1), 812–837 (2018)
20. Wang, S., Wu, J., Yang, W., Guo, L.-H.: Novel architectures and security solutions of programmable software-defined networking: a comprehensive survey. Front. Inf. Technol. Electron. Eng. **19**(12), 1500–1521 (2018)
21. Berdik, D., Otoum, S., Schmidt, N., Porter, D., Jararweh, Y.: A survey on blockchain for information systems management and security. Inf. Process. Manag. **58**(1), 102397 (2021)
22. Bhutta, M.N.M., Khwaja, A.A., Nadeem, A., Ahmad, H.F., Khan, M.K., Hanif, M.A., Song, H., Alshamari, M., Cao, Y.: A survey on blockchain technology: evolution, architecture and security. IEEE Access **9**, 61048–61073 (2021)
23. Hewa, T.M., Hu, Y., Liyanage, M., Kanhare, S., Ylianttila, M.: Survey on blockchain based smart contracts: technical aspects and future research. IEEE Access **9**, 87643–87662 (2021)
24. Yue, K., Zhang, Y., Chen, Y., Li, Y., Zhao, L., Rong, C., Chen, L.: A survey of decentralizing applications via blockchain: the 5G and beyond perspective. IEEE Commun. Surv. Tutor. **23**(4), 1 (2021)
25. Latif, S., Idrees, Z., e Huma, Z., Ahmad, J.: Blockchain technology for the Industrial Internet of Things: a comprehensive survey on security challenges, architectures, applications, and future research directions. Trans. Emerg. Telecommun. Technol. **32**(4), e4337 (2021)
26. Da Xu, L., Lu, Y., Li, L.: Embedding blockchain technology into IoT for security: a survey. IEEE Internet Things J. **8**(13), 10452–10473 (2021)
27. Ahmed, S.: Chapter three blockchain and Industry 4.0. In: Ahmed, S., Khan, R.H. (eds) Blockchain in Data Analytics, vol. 52. Cambridge Scholars Publishing, Cambridge (2020)
28. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Future Gener. Comput. Syst. **107**, 841–853 (2020)
29. Sengupta, J., Ruj, S., Bit, S.D.: A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Netw. Comput. Appl. **149**, 102481 (2020)
30. Dasgupta, D., Shrein, J.M., Gupta, K.D.: A survey of blockchain from security perspective. J. Bank. Financ. Technol. **3**(1), 1–17 (2019)
31. Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N.: A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. **126**, 45–58 (2019)
32. Gao, W., Hatcher, W.G., Yu, W.: A survey of blockchain: techniques, applications, and challenges. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–11. IEEE (2018)
33. Nguyen, G.-T., Kim, K.: A survey about consensus algorithms used in blockchain. J. Inf. Process. Syst. **14**(1), 101–128 (2018)
34. Salman, T., Zolanvari, M., Erbad, A., Jain, R., Samaka, M.: Security services using blockchains: a state of the art survey. IEEE Commun. Surv. Tutor. **21**(1), 858–880 (2018)
35. Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., Janicke, H.: Blockchain technologies for the Internet of Things: research issues and challenges. IEEE Internet Things J. **6**(2), 2188–2204 (2018)
36. Banerjee, M., Lee, J., Choo, K.-K.R.: A blockchain future for Internet of Things security: a position paper. Digit. Commun. Netw. **4**(3), 149–160 (2018)
37. Barakabitze, A.A., Ahmad, A., Mijumbi, R., Hines, A.: 5G network slicing using SDN and NFV: a survey of taxonomy, architectures and future challenges. Comput. Netw. **167**, 106984 (2020)

38. Bannour, F., Souihi, S., Mellouk, A.: Distributed SDN control: survey, taxonomy, and challenges. IEEE Commun. Surv. Tutor. **20**(1), 333–354 (2017)
39. Iqbal, M., Iqbal, F., Mohsin, F., Rizwan, M., Ahmad, F.: Security issues in software defined networking (SDN): risks, challenges and potential solutions. Int. J. Adv. Comput. Sci. Appl. (2019). https://doi.org/10.14569/IJACSA.2019.0101042
40. Bizanis, N., Kuipers, F.A.: SDN and virtualization solutions for the Internet of Things: a survey. IEEE Access **4**, 5591–5606 (2016)
41. Karakus, M., Durresi, A.: A survey: control plane scalability issues and approaches in software-defined networking (SDN). Comput. Netw. **112**, 279–293 (2017)
42. Iqbal, W., Abbas, H., Rauf, B., Abbas, Y., Amjad, F., Hemani, A.: PCSS: privacy preserving communication scheme for SDN enabled smart homes. IEEE Sens. J. (2021). https://doi.org/10.1109/JSEN.2021.3087779
43. Rahman, A., Chakraborty, C., Anwar, A., Karim, M., Islam, M., Kundu, D., Rahman, Z., Band, S.S., et al.: SDN–IoT empowered intelligent framework for Industry 4.0 applications during COVID-19 pandemic. Clust. Comput. **25**, 1–18 (2021)
44. Tariq, F., Anwar, M., Janjua, A.R., Khan, M.H., Khan, A.U., Javaid, N.: Blockchain in WSNs, VANETs, IoTs and healthcare: a survey. In: Workshops of the International Conference on Advanced Information Networking and Applications, pp. 267–279. Springer (2020)
45. Deepa, N., Pham, Q.-V., Nguyen, D.C., Bhattacharya, S., Gadekallu, T.R., Maddikunta, P.K.R., Fang, F., Pathirana, P.N., et al.: A survey on blockchain for big data: approaches, opportunities, and future directions. arXiv preprint (2020). arXiv:2009.00858
46. Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y.: Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput. Appl. **34**, 1–16 (2021)
47. Dai, H.-N., Zheng, Z., Zhang, Y.: Blockchain for Internet of Things: a survey. IEEE Internet Things J. **6**(5), 8076–8094 (2019)
48. Wadhwa, S., Babbar, H., Rani, S.: A survey on emerging software-defined networking and blockchain in smart health care. IOP Conf. Ser. Mater. Sci. Eng. **1022**, 012056 (2021)
49. Hassan, H.A., Hemdan, E.E., El-Shafai, W., Shokair, M., Abd El-Samie, F.E.: A survey on SDN-based intrusion detection systems on the Internet of Things: concepts, issues, and blockchain applications. Wirel. Pers. Commun. (2021). https://doi.org/10.21203/rs.3.rs-694000/v1
50. Alharbi, T.: Deployment of blockchain technology in software defined networks: a survey. IEEE Access **8**, 9146–9156 (2020)
51. Rahman, A., Islam, M.J., Rahman, Z., Reza, M.M., Anwar, A., Mahmud, M.P., Nasir, M.K., Noor, R.M.: DistB-Condo: distributed blockchain-based IoT-SDN model for smart condominium. IEEE Access **8**, 209594–209609 (2020)
52. Joshi, A.P., Han, M., Wang, Y.: A survey on security and privacy issues of blockchain technology. Math. Found. Comput. **1**(2), 121–147 (2018)
53. Antonopoulos, A.M.: Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media, Inc., Sebastopol (2017)
54. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 3–16. ACM (2016)
55. Ali, S.T., Sivaraman, V., Radford, A., Jha, S.: A survey of securing networks using software defined networking. IEEE Trans. Reliab. **64**(3), 1086–1097 (2015)
56. Megyesi, P., Botta, A., Aceto, G., Pescapè, A., Molnár, S.: Challenges and solution for measuring available bandwidth in software defined networks. Comput. Commun. **99**, 48–61 (2017)
57. Ali, S., Alvi, M.K., Faizullah, S., Khan, M.A., Alshanqiti, A., Khan, I.: Detecting DDoS attack on SDN due to vulnerabilities in OpenFlow. In: 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), pp. 1–6 (2020)
58. Shaghaghi, A., Kaafar, M.A., Buyya, R., Jha, S.: Software-defined network (SDN) data plane security: issues, solutions, and future directions. In: Handbook of Computer Networks and Cyber Security, pp. 341–387. Springer, Cham (2020)
59. Abuarqoub, A.: A review of the control plane scalability approaches in software defined networking. Future Internet **12**(3), 49 (2020)
60. Cui, L., Yu, F.R., Yan, Q.: When big data meets software-defined networking: SDN for big data and big data for SDN. IEEE Netw. **30**(1), 58–65 (2016)

61. Rahman, A., Nasir, M.K., Rahman, Z., Mosavi, A., Shahab, S., Minaei-Bidgoli, B.: DistBlock-Building: a distributed blockchain-based SDN–IoT network for smart building management. IEEE Access **8**, 140008–140018 (2020)
62. Pritchard, S.W., Hancke, G.P., Abu-Mahfouz, A.M.: Security in software-defined wireless sensor networks: threats, challenges and potential solutions. In: 2017 IEEE 15th International Conference on Industrial Informatics (INDIN), pp. 168–173. IEEE (2017)
63. Ourad, A.Z., Belgacem, B., Salah, K.: Using blockchain for IoT access control and authentication management. In: International Conference on Internet of Things, pp. 150–164. Springer (2018)
64. Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A.: Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Comput. Secur. **78**, 126–142 (2018)
65. Lin, C., He, D., Huang, X., Choo, K.-K.R., Vasilakos, A.V.: BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for Industry 4.0. J. Netw. Comput. Appl. **116**, 42–52 (2018)
66. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., Santamaría, V.: Blockchain and smart contracts for insurance: is the technology mature enough? Future Internet **10**(2), 20 (2018)
67. Sharma, P.K., Singh, S., Jeong, Y.-S., Park, J.H.: DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun. Mag. **55**(9), 78–85 (2017)
68. El Houda, Z.A., Hafid, A.S., Khoukhi, L.: Cochain-SC: an intra- and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract. IEEE Access **7**, 98893–98907 (2019)
69. Muthanna, A., Ateya, A.A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., Koucheryavy, A.: Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. J. Sens. Actuator Netw. **8**(1), 15 (2019)
70. Zhang, D., Yu, F.R., Yang, R.: Blockchain-based distributed software-defined vehicular networks: a dueling deep $*q* $-learning approach. IEEE Trans. Cogn. Commun. Netw. **5**(4), 1086–1100 (2019)
71. Navid Rajabi, J.Q.: SDIoBoT: a software-defined internet of blockchains of things model. Int. J. Internet Things **8**, 17–26 (2019)
72. Derhab, A., Guerroumi, M., Gumaei, A., Maglaras, L., Ferrag, M.A., Mukherjee, M., Khan, F.A.: Blockchain and random subspace learning-based IDs for SDN-enabled industrial IoT security. Sensors **19**(14), 3119 (2019)
73. Sharma, P.K., Chen, M.-Y., Park, J.H.: A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access **6**, 115–124 (2017)
74. Xie, L., Ding, Y., Yang, H., Wang, X.: Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. IEEE Access **7**, 56656–56666 (2019)
75. Gao, J., Agyekum, K.O.-B.O., Sifah, E.B., Acheampong, K.N., Xia, Q., Du, X., Guizani, M., Xia, H.: A blockchain-SDN-enabled Internet of Vehicles environment for fog computing and 5G networks. IEEE Internet Things J. **7**(5), 4278–4291 (2019)
76. Chaudhary, R., Jindal, A., Aujla, G.S., Aggarwal, S., Kumar, N., Choo, K.-K.R.: BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. Comput. Secur. **85**, 288–299 (2019)
77. Zhiyi, L., Shahidehpour, M., Xuan, L.: Cyber-secure decentralized energy management for IoT-enabled active distribution networks. J. Mod. Power Syst. Clean Energy **6**(5), 900–917 (2018)
78. Fernando, P., Wei, J.: Blockchain-powered software defined network-enabled networking infrastructure for cloud management. In: 2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC), pp. 1–6 (2020)
79. Qiu, C., Yu, F.R., Xu, F., Yao, H., Zhao, C.: Permissioned blockchain-based distributed software-defined Industrial Internet of Things. In: 2018 IEEE GLOBECOM Workshops (GC Wkshps), pp. 1–7. IEEE (2018)
80. Shao, Z., Zhu, X., Chikuvanyanga, A.M., Zhu, H.: Blockchain-based SDN security guaranteeing algorithm and analysis model. In: International Conference on Wireless and Satellite Systems, pp. 348–362. Springer (2019)
81. Liu, Y., Zhao, B., Li, X., Wang, S., Zhang, B., Liu, Z.: A trust chain assessment method based on blockchain for SDN network nodes. In: 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), pp. 240–245. IEEE (2019)
82. Tselios, C., Politis, I., Kotsopoulos, S.: Enhancing SDN security for IoT-related deployments through blockchain. In: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV–SDN), pp. 303–308. IEEE (2017)

83. Basnet, S.R., Shakya, S.: BSS: Blockchain security over software defined network. In: 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 720–725. IEEE (2017)
84. Kataoka, K., Gangwar, S., Podili, P.: Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 296–301. IEEE (2018)
85. Steichen, M., Hommes, S., State, R.: ChainGuard—a firewall for blockchain applications using SDN with OpenFlow. In: 2017 Principles, Systems and Applications of IP Telecommunications (IPTComm), pp. 1–8. IEEE (2017)
86. Abou El Houda, Z., Hafid, A., Khoukhi, L.: Co-IoT: a collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2019)
87. Okon, A.A., Elgendi, I., Sholiyi, O.S., Elmirghani, J.M., Jamalipour, A., Munasinghe, K.: Blockchain and SDN architecture for spectrum management in cellular networks. IEEE Access **8**, 94415–94428 (2020)
88. Wang, H., Wang, Y., Cao, Z., Li, Z., Xiong, G.: An overview of blockchain security analysis. In: China Cyber Security Annual Conference, pp. 55–72. Springer (2018)
89. Lin, I.-C., Liao, T.-C.: A survey of blockchain security issues and challenges. IJ Netw. Secur. **19**(5), 653–659 (2017)
90. Peltier, T.R.: Social engineering: concepts and solutions. Inf. Secur. J. **15**(5), 13 (2006)
91. LedgerOps (2019). https://ledgerops.com/blog/2019/03/28/top-five-blockchain-security-issues-in-2019/
92. Rahman, A., Islam, M.J., Montieri, A., Nasir, M.K., Reza, M.M., Band, S.S., Pescape, A., Hasan, M., Sookhak, M., Mosavi, A.: SmartBlock-SDN: an optimized blockchain-SDN framework for resource management in IoT. IEEE Access **9**, 28361–28376 (2021)
93. Li, W., Guo, H., Nejad, M., Shen, C.-C.: Privacy-preserving traffic management: a blockchain and zero-knowledge proof inspired approach. IEEE Access **8**, 181733–181743 (2020)
94. Yu, Y., Li, Y., Tian, J., Liu, J.: Blockchain-based solutions to security and privacy issues in the Internet of Things. IEEE Wirel. Commun. **25**(6), 12–18 (2018)
95. Mohanta, B.K., Jena, D., Ramasubbareddy, S., Daneshmand, M., Gandomi, A.H.: Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet Things J. **8**(2), 881–888 (2020)
96. Zhang, R., Xue, R., Liu, L.: Security and privacy on blockchain. ACM Comput. Surv. **52**(3), 1–34 (2019)
97. Shi, S., He, D., Li, L., Kumar, N., Khan, M.K., Choo, K.-K.R.: Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. Comput. Secur. **97**, 101966 (2020)
98. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564. IEEE (2017)
99. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. **88**, 173–190 (2018)
100. Pazmiño, J.E., Rodrigues, C.: Simply dividing a Bitcoin network node may reduce transaction verification time. SIJ Trans. Comput. Netw. Commun. Eng. **3**(2), 17–21 (2015)
101. Zkik, K., El Hajji, S., Orhanou, G.: Design and implementation of a new security plane for hybrid distributed SDNs. J. Commun. **14**(1), 26–32 (2019)
102. Chica, J.C.C., Imbachi, J.C., Botero, J.F.: Security in SDN: a comprehensive survey. J. Netw. Comput. Appl. **159**, 102595 (2020)
103. Lee, S., Kim, J., Shin, S., Porras, P., Yegneswaran, V.: Athena: a framework for scalable anomaly detection in software-defined networks. In: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 249–260. IEEE (2017)
104. Islam, M.J., Rahman, A., Kabir, S., Khatun, A., Pritom, A., Chowdhury, M.: SDoT-NFV: a distributed SDN based security system with IoT for smart city environments. GUB J. Sci. Eng. **7**, 27–35 (2021)
105. Shamshirband, S., Fathi, M., Chronopoulos, A.T., Montieri, A., Palumbo, F., Pescapè, A.: Computational intelligence intrusion detection techniques in mobile cloud computing environments: review, taxonomy, and open research issues. J. Inf. Secur. Appl. **55**, 102582 (2020)

106. Yang, L., Zhao, H.: DDoS attack identification and defense using SDN based on machine learning method. In: 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN), pp. 174–178. IEEE (2018)
107. Islam, S., Sara, U., Kawsar, A., Rahman, A., Kundu, D., Dipta, D.D., Karim, A.R., Hasan, M.: SGBBA: an efficient method for prediction system in machine learning using imbalance dataset. Int. J. Adv. Comput. Sci. Appl. (2021). https://doi.org/10.14569/IJACSA.2021.012035
108. Khattak, H.A., Tehreem, K., Almogren, A., Ameer, Z., Din, I.U., Adnan, M.: Dynamic pricing in Industrial Internet of Things: Blockchain application for energy management in smart cities. J. Inf. Secur. Appl. **55**, 102615 (2020)
109. Thangavel, M., Pavithra, V., Guru Roja, R.: Network manipulation using network scanning in SDN. In: Artificial Intelligence and Security Challenges in Emerging Networks, pp. 85–123. IGI Global, Pennsylvania (2019)
110. Priya, A.V., Singh, H.K.: Mitigation of ARP cache poisoning in software-defined networks. In: Advances in Smart System Technologies, pp. 85–94. Springer, Singapore (2021)
111. Gadze, J.D., Bamfo-Asante, A.A., Agyemang, J.O., Nunoo-Mensah, H., Opare, K.A.-B.: An investigation into the application of deep learning in the detection and mitigation of DDoS attack on SDN controllers. Technologies **9**(1), 14 (2021)
112. Altarawneh, A., Sun, F., Brooks, R.R., Hambolu, O., Yu, L., Skjellum, A.: Availability analysis of a permissioned blockchain with a lightweight consensus protocol. Comput. Secur. **102**, 102098 (2021)
113. Aceto, G., Botta, A., Marchetta, P., Persico, V., Pescapè, A.: A comprehensive survey on Internet outages. J. Netw. Comput. Appl. **113**, 36–63 (2018)
114. Fitwi, A., Chen, Y., Zhu, S.: A lightweight blockchain-based privacy protection for smart surveillance at the edge. In: 2019 IEEE International Conference on Blockchain (Blockchain), pp. 552–555. IEEE (2019)
115. Li, C.Z., Chen, Z., Xue, F., Kong, X.T., Xiao, B., Lai, X., Zhao, Y.: A blockchain- and IoT-based smart product–service system for the sustainability of prefabricated housing construction. J. Clean. Prod. **286**, 125391 (2021)
116. Kouhizadeh, M., Saberi, S., Sarkis, J.: Blockchain technology and the sustainable supply chain: theoretically exploring adoption barriers. Int. J. Prod. Econ. **231**, 107831 (2021)
117. Islam, M.J., Rahman, A., Kabir, S., Karim, M.R., Acharjee, U.K., Nasir, M.K., Band, S.S., Sookhak, M., Wu, S.: Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities. IEEE Internet Things J. **9**(5), 3850–3864 (2022)
118. Hamledari, H., Fischer, M.: The application of blockchain-based crypto assets for integrating the physical and financial supply chains in the construction & engineering industry. Autom. Constr. **127**, 103711 (2021)
119. Hong, W., Mao, J., Wu, L., Pu, X.: Public cognition of the application of blockchain in food safety management—data from China's Zhihu platform. J. Clean. Prod. **303**, 127044 (2021)
120. Mishra, L., Kaushik, V.: Application of blockchain in dealing with sustainability issues and challenges of financial sector. J. Sustain. Finance Invest. (2021). https://doi.org/10.1080/20430795.2021.1940805
121. Rahman, A., Islam, M.J., Karim, M.R., Kundu, D., Kabir, S.: An intelligent vaccine distribution process in COVID-19 pandemic through blockchain-SDN framework from Bangladesh perspective. In: 2021 International Conference on Electronics, Communications and Information Technology (ICECIT), pp. 1–4 (2021)
122. Kabir, M.R., Islam, M.A., Marniati, Herawati: Application of blockchain for supply chain financing: explaining the drivers using SEM. J. Open Innov. Technol. Market Complex. **7**(3), 167 (2021)
123. Hossain, M.J., Wadud, M.A.H., Rahman, A., Ferdous, J., Alam, M.S., Amir Ul Haque Bhuiyan, T.M., Mridha, M.F.: A secured patient's online data monitoring through blockchain: an intelligent way to store lifetime medical records. In: 2021 International Conference on Science Contemporary Technologies (ICSCT), pp. 1–6 (2021)
124. Pan, X., Pan, X., Song, M., Ai, B., Ming, Y.: Blockchain technology and enterprise operational capabilities: an empirical test. Int. J. Inf. Manag. **52**, 101946 (2020)
125. Tönnissen, S., Teuteberg, F.: Analysing the impact of blockchain-technology for operations and supply chain management: an explanatory model drawn from multiple case studies. Int. J. Inf. Manag. **52**, 101953 (2020)

126. Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., Irani, Z.: A framework for analysing blockchain technology adoption: integrating institutional, market and technical factors. Int. J. Inf. Manag. **50**, 302–309 (2020)
127. Xu, Q., He, Z., Li, Z., Xiao, M., Goh, R.S.M., Li, Y.: An effective blockchain-based, decentralized application for smart building system management. In: Real-Time Data Analytics for Large Scale Sensor Data, pp. 157–181. Elsevier, Amsterdam (2020)
128. Rahman, A., Islam, M.J., Saikat Islam Khan, M., Kabir, S., I. Pritom, A., Razaul Karim, M.: Block-SDoTcloud: enhancing security of cloud storage through blockchain-based SDN in IoT network. In: 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), pp. 1–6 (2020)
129. Nawari, N.O., Ravindran, S.: Blockchain and building information modeling (BIM): review and applications in post-disaster recovery. Buildings **9**(6), 149 (2019)
130. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., Wang, F.-Y.: Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans. Syst. Man Cybern. **49**(11), 2266–2277 (2019)
131. Lu, H., Huang, K., Azimi, M., Guo, L.: Blockchain technology in the oil and gas industry: a review of applications, opportunities, challenges, and risks. IEEE Access **7**, 41426–41444 (2019)
132. Tijan, E., Aksentijević, S., Ivanić, K., Jardas, M.: Blockchain technology implementation in logistics. Sustainability **11**(4), 1185 (2019)
133. Rahman, A., Islam, M.J., Sunny, F.A., Nasir, M.K.: DistBlockSDN: a distributed secure blockchain based SDN–IoT architecture with NFV implementation for smart cities. In: 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), pp. 1–6 (2019)
134. Aggarwal, S., Chaudhary, R., Aujla, G.S., Kumar, N., Choo, K.-K.R., Zomaya, A.Y.: Blockchain for smart communities: applications, challenges and opportunities. J. Netw. Comput. Appl. **144**, 13–48 (2019)
135. Cha, S.-C., Chen, J.-F., Su, C., Yeh, K.-H.: A blockchain connected gateway for BLE-based devices in the Internet of Things. IEEE Access **6**, 24639–24649 (2018)
136. Zhang, Q., Novotny, P., Baset, S., Dillenberger, D., Barger, A., Manevich, Y.: LedgerGuard: improving blockchain ledger dependability. In: International Conference on Blockchain, pp. 251–258. Springer (2018)
137. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. **42**(7), 130 (2018)
138. Swati, V., Prasad, A.S.: Application of blockchain technology in travel industry. In: 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), pp. 1–5. IEEE (2018)
139. Cheng, J.-C., Lee, N.-Y., Chi, C., Chen, Y.-H.: Blockchain and smart contract for digital certificate. In: 2018 IEEE International Conference on Applied System Invention (ICASI), pp. 1046–1051. IEEE (2018)
140. Ghazali, O., Saleh, O.S.: A graduation certificate verification model via utilization of the blockchain technology. J. Telecommun. Electron. Comput. Eng. **10**(3–2), 29–34 (2018)
141. Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., Wendland, F.: Blockchain for education: lifelong learning passport. In: Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET) (2018)
142. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards an optimized blockchain for IoT. In: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 173–178. IEEE (2017)
143. Aras, S.T., Kulkarni, V.: Blockchain and its applications—a detailed survey. Int. J. Comput. Appl. **180**(3), 29–35 (2017)
144. Pass, R., Shi, E.: FruitChains: a fair blockchain. In: Proceedings of the ACM Symposium on Principles of Distributed Computing, pp. 315–324 (2017)
145. Sharples, M., Domingue, J.: The blockchain and kudos: a distributed system for educational record, reputation and reward. In: European Conference on Technology Enhanced Learning, pp. 490–496. Springer (2016)
146. Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. **5**(9), 1–10 (2016)

147. Francisco, K., Swanson, D.: The supply chain has no clothes: technology adoption of blockchain for supply chain transparency. Logistics **2**(1), 2 (2018)
148. Yavuz, E., Koc, A.K., Çabuk, U.C., Dalkılıç, G.: Towards secure e-voting using Ethereum blockchain. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1–7. IEEE (2018)
149. Pareek, S., Upadhyay, A., Doulani, S., Tyagi, S., Varma, A.: E-voting using Ethereum blockchain. IJRTI **3**, 2456–3315 (2018)
150. Wang, Z., Jin, H., Dai, W., Choo, K.-K.R., Zou, D.: Ethereum smart contract security research: survey and future research opportunities. Front. Comput. Sci. **15**(2), 1–18 (2021)
151. Sankaran, S., Sanju, S., Achuthan, K.: Towards realistic energy profiling of blockchains for securing Internet of Things. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pp. 1454–1459. IEEE (2018)
152. Rahman, A., Rahman, M., Kundu, D., Karim, M.R., Band, S.S., Sookhak, M.: Study on IoT for SARS-CoV-2 with healthcare: present and future perspective. Math. Biosci. Eng. **18**(6), 9697–9726 (2021)
153. Bovenzi, G., Aceto, G., Ciuonzo, D., Persico, V., Pescapè, A.: A hierarchical hybrid intrusion detection approach in IoT scenarios. In: IEEE Global Communications Conference, GLOBECOM 2020, Virtual Event, Taiwan, 7–11 December 2020, pp. 1–7. IEEE (2020)
154. Nascita, A., Cerasuolo, F., Di Monda, D., Garcia, J., Montieri, A., Pescapè, A.: Machine and deep learning approaches for IoT attack classification. In: IEEE INFOCOM Workshops'22, 05 (2022)
155. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623 (2017)
156. Hasan, M., Rahman, A., Islam, M.J.: DistB-CVS: a distributed secure blockchain based online certificate verification system from Bangladesh perspective. In: 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT), pp. 460–465 (2020)
157. Rahman, A., Sara, U., Kundu, D., Islam, S., Islam, M.J., Hasan, M., Rahman, Z., Nasir, M.K.: DistB-SDoIndustry: enhancing security in Industry 4.0 services based on distributed blockchain through software defined networking-IoT enabled architecture. Int. J. Adv. Comput. Sci. Appl. **11**, 9 (2020)
158. Zuo, Y.: Making smart manufacturing smarter—a survey on blockchain technology in Industry 4.0. Enterp. Inf. Syst. **15**(10), 1–31 (2020)
159. Yan, Y., Duan, B., Zhong, Y., Qu, X.: Blockchain technology in the Internet plus: the collaborative development of power electronic devices. In: IECON 2017—43rd Annual Conference of the IEEE Industrial Electronics Society, pp. 922–927. IEEE (2017)
160. Sittón-Candanedo, I.: A new approach: edge computing and blockchain for Industry 4.0. In: International Symposium on Distributed Computing and Artificial Intelligence, pp. 201–204. Springer (2019)
161. Fernández-Caramés, T.M., Blanco-Novoa, O., Froiz-Míguez, I., Fraga-Lamas, P.: Towards an autonomous Industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. Sensors **19**(10), 2394 (2019)
162. Misra, S., Deb, P.K., Pathak, N., Mukherjee, A.: Blockchain-enabled SDN for securing fog-based resource-constrained IoT. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 490–495. IEEE (2020)
163. Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Zhang, Q., Choo, K.-K.R.: An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Trans. Serv. Comput. **13**(4), 625–638 (2020)
164. Qiu, C., Yu, F.R., Yao, H., Jiang, C., Xu, F., Zhao, C.: Blockchain-based software-defined industrial Internet of Things: a dueling deep Q-learning approach. IEEE Internet Things J. **6**(3), 4627–4639 (2018)
165. Shayshab Azad, K.M., Hossain, N., Islam, M.J., Rahman, A., Kabir, S.: Preventive determination and avoidance of DDoS attack with SDN over the IoT networks. In: 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), pp. 1–6 (2021)
166. Zaman, S., Khandaker, M.R., Khan, R.T., Tariq, F., Wong, K.-K.: Thinking out of the blocks: Holochain for distributed security in IoT healthcare. arXiv preprint (2021). arXiv:2103.01322

167. Janjua, K., Shah, M.A., Almogren, A., Khattak, H.A., Maple, C., Din, I.U.: Proactive forensics in IoT: privacy-aware log-preservation architecture in fog-enabled-cloud using Holochain and containerization technologies. Electronics **9**(7), 1172 (2020)
168. Aceto, G., Ciuonzo, D., Montieri, A., Pescapé, A.: Mobile encrypted traffic classification using deep learning: experimental evaluation, lessons learned, and challenges. IEEE Trans. Netw. Serv. Manag. **16**(2), 445–458 (2019)
169. Bovenzi, G., Cerasuolo, F., Montieri, A., Nascita, A., Persico, V., Pescapé, A.: A comparison of machine and deep learning models for detection and classification of android malware traffic. In: IEEE DistInSys'22 (2022)



**Anichur Rahman** received the B.Sc. and M.Sc Degrees in Computer Science and Engineering from Mawlana Bhashani Science and Technology University, Bangladesh in 2017 and 2020 respectively. Currently, he is working as a Lecturer at Computer Science and Engineering National Institute of Textile Engineering and Research, Bangladesh. His research interests include the Internet of Things, Blockchain, Software Defined Networking, Machine Learning, 5G, Industry 4.0, and Data Science.

**Antonio Montieri** is an Assistant Professor at DIETI of the University of Napoli Federico II. He has received his Ph.D. Degree in Information Technology and Electrical Engineering in April 2020 from the same University. His work concerns network measurements, (encrypted and mobile) traffic classification, traffic modeling and prediction, and monitoring of cloud network performance. Antonio has co-authored 35 papers in international journals and conference proceedings.

**Dipanjali Kundu** received the B.Sc. Degree in Computer Science and Engineering from Chittagong University of Engineering and Technology, Bangladesh in 2018. Currently, she is working as a Lecturer at Computer Science and Engineering, National Institute of Textile Engineering and Research, Bangladesh. Her research interests include Machine Learning, Human Computer Interaction, Internet of Things, Blockchain, Software Defined Networking, 5G, Industry 4.0, and Robotics.

**Md. Razaul Karim** received the B.Sc. Degree in Computer Science and Engineering from Mawlana Bhashani Science and Technology University, Tangail, Bangladesh in 2020. The main interests of his research are Machine Learning, Computer Vision, and Image Processing. He is also keen on Blockchain.

**Md. Jahidul Islam** received the B.Sc. and M.Sc. Degrees in Computer Science and Engineering from Jagannath University, Dhaka, in 2015 and 2017 respectively. Currently, he is working as a Lecturer and Program Coordinator at Computer Science and Engineering, Green University of Bangladesh. His research interests include Internet of Things, Blockchain, Network Function Virtualization, Software Defined Networking, 5G, Industry 4.0, Machine Learning, and Wireless Mesh Networking.

**Sara Umme** received her B.Sc. in 2012 and M.Sc. in 2014 both from the Jahangirnager University under the Discipline of Computer Science and Engineering. Currently, she is working as an Assistant Professor and Head at the Department of Computer Science and Engineering, National Institute of Textile Engineering and Research, Bangladesh. Her current research interests include Machine Learning, Digital Image Processing, Computer Vision Systems, Data Science, IoT, and Blockchain.

**Alfredo Nascita** is a Ph.D. Student in Information Technology and Electrical Engineering at DIETI, University of Napoli Federico II. He received his M.S. Laurea Degree in Computer Engineering from the same University in March 2021. His research interests include traffic classification, machine and deep learning, and explainable artificial intelligence.

**Antonio Pescapé** is a Full Professor of Computer Engineering at the University of Napoli Federico II. His work focuses on measurement, monitoring, and analysis of the Internet. He has co-authored more than 200 conference and journal papers, he is the recipient of a number of research awards. Also, he has

served as an independent reviewer/evaluator of research projects/project proposals co-funded by a number of governments and agencies.

## Authors and Affiliations

**Anichur Rahman[1] · Antonio Montieri[2] · Dipanjali Kundu[1] · Md. Razaul Karim[3] · Md. Jahidul Islam[4] · Sara Umme[1] · Alfredo Nascita[2] · Antonio Pescapé[2]**

Anichur Rahman
anis_cse@niter.edu.bd

Dipanjali Kundu
dipanjali_kundu@niter.edu.bd

Md. Razaul Karim
razaulce15004@gmail.com

Md. Jahidul Islam
jahidul.jnucse@gmail.com

Sara Umme
ummesara@niter.edu.bd

Alfredo Nascita
alfredo.nascita@unina.it

Antonio Pescapé
pescape@unina.it

1 Department of Computer Science and Engineering, National Institute of Textile Engineering and Research (NITER), Constituent Institute of Dhaka University, Savar, Dhaka 1350, Bangladesh

2 University of Napoli Federico II, Naples, Italy

3 Mawlana Bhashani Science and Technology University, Tangail, Bangladesh

4 Green University of Bangladesh, Dhaka, Bangladesh