IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 10, 2019, accepted December 26, 2019, date of publication January 8, 2020, date of current version January 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2964751

Deployment of Blockchain Technology in Software Defined Networks: A Survey

TALAL ALHARBI
Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majma'ah 11952, Saudi Arabia
e-mail: talal@mu.edu.sa

This work was supported by the Deanship of Scientific Research at Majmaah University under Project R-1441-58.

ABSTRACT With the exponential increase in the complexity of network management and configuration, Software Defined Networking (SDN) has emerged as a promising network paradigm. SDN aims to efficiently transform network architecture and operations to be agile, and effectively enrich the functionality of underlying network elements, such as routers and switches, by decoupling the control plane from the data plane. In SDN, the network intelligence is centralized in a software entity so-called SDN controller, which enables network administrators to dynamically manage, secure, and optimize network resources and programmatically shape all entire network traffic pattern. Despite the impressive benefits SDN has brought to network architecture, it introduces new security challenges and prompts different implementation strategies to spread attack vectors. This paper comprehensively describes the utilization of Blockchain technology to secure and protect SDN architecture and discusses the feasibility of integrating the revolutionary technologies of SDN and Blockchain to provide confidentiality, integrity, and availability to network infrastructure.

INDEX TERMS Blockchain, Bitcoin, SDN, OpenFlow, cybersecurity, network security.

I. INTRODUCTION

When the demand for online banking and financial services increased, Blockchain technology was introduced as a disruptive technology to essentially build a secure online payment system with no need for financial institutions. The technology has received extensive attentions from different communities, including scholars, industries, and stakeholders, and has made big waves by realizing Bitcoin, the world's most popular cryptocurrency [1].

Due to the striking characteristics of Blockchain, including decentralization, anonymity, persistency, and audibility, the technology has been widely adopted and spread among various sectors, such as healthcare, finance, smart contracts, and Internet of Things (IoT). [2]–[5]. The global Blockchain market size has grown exponentially and is expected to be worth over 23.3 billion U.S. dollars by 2023, as shown in Figure 1. The key factors that drive this market are the simplicity and transparency of the business process between the sender and receiver in Blockchain technology. However, the business process is traditionally handled and managed via a third party organization, which requires a significant amount of time to complete transactions between parties and typically charges for incoming and outgoing wire transfers.

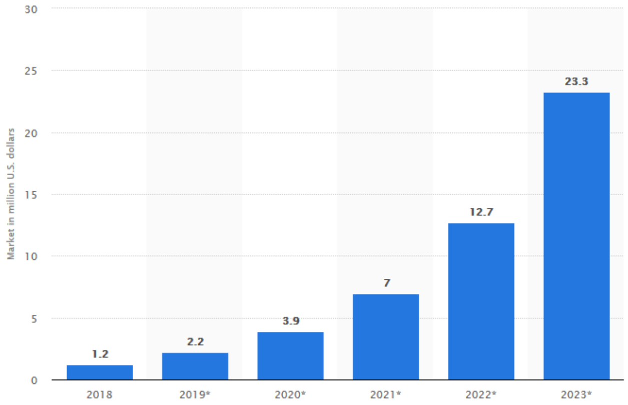

FIGURE 1. Blockchain technology market size [6].

Blockchain appears to be the driving technology leading to a massive revolution in the internet space [7]. Figure 2 summrizes the digital revelution of Blockchain based on information provided in [8]–[12]. The technology is useful, especially in the banking industry, because Blockchain transactions are immutable and non-reversible, i.e. cannot to be tampered with, resulting in attracting individuals who seek

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

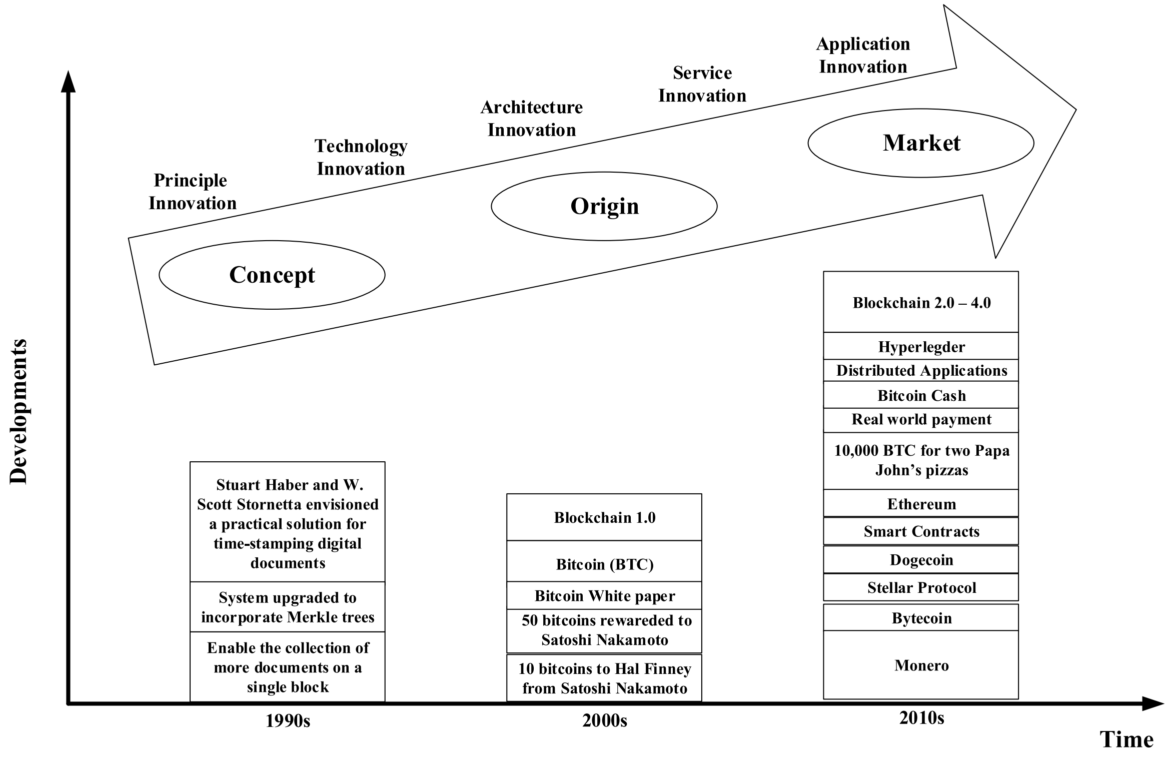

FIGURE 2. The evolution of Blockchain technology.

reliability and honesty when there is no trusted third party involved to manage the digital transactions. Thus, transaction fees and time required for money transfer across multiple enterprise boundaries are significantly reduced compared to normal operation.

The elimination of a central authority and storage location makes Blockchain a powerful weapon to defeat the most common and disruptive attack in transitional networks, i.e the Distributed Denial of Service Attack (DDoS), in which the attackers explicitly flood the network attempting to prevent legitimate users from accessing network resources [13]. For instance, Blockstack is built on top of Blockchain technology to fully decentralize the worldwide web, where in this case, third parties are no longer responsible for the management of web servers and databases [14].

The complete opposite of Blockchain technology is Software Defined Networking (SDN), where network management and configuration are centralized in a software entity, i.e. SDN controller. The SDN architecture has tackled few security issues that exist in traditional networks through the separation of the data plane from the control plane, while it introduces new attack vectors [15]. Distributing some network functionalities in a method similar to the implementation of Blockchain technology might enhance security vulnerabilities in the SDN architecture.

Therefore, in this paper, we focus on analyzing the current implementation of Blockchain technology in SDN for security purposes and address the limitations of proposed solutions. Our main contributions can be summarized as follows:

- We provide preliminary details about Blockchain and SDN.
- We analyze existing studies relating to the deployment of Blockchain Technology in SDN and summarize their findings.
- We identify new challenges and issues raised from proposed solutions and discuss potential research directions to secure SDN using different Blockchain applications.

The remainder of this paper is organized as follows: Section II provides a brief overview of Blockchain technology and SDN. Section III discusses the findings in more detail, and Section IV suggests the future work based on the limitations of current proposed solutions. Section V concludes the paper.

II. BACKGROUND

In this section, we discuss the basic concepts presented in this paper related to Blockchain technology and SDN. We provide great detail on how those technologies work and how they can be integrated.

A. BLOCKCHAIN TECHNOLOGY

Blockchain is essentially a data management technology that stores a complete list of committed transactions and digital events in a sequence of blocks managed via a cluster of computers rather than a single entity [1]. These computers are connected to each other over a peer-to-peer (P2P) network and each node (block) contains three elements: data, a hash value, and the hash value of the previous block, as shown

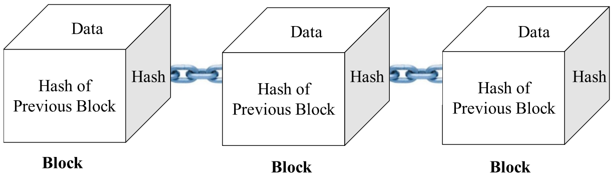

FIGURE 3. Blockchain architecture.

in Figure 3. The data stored in each block contains the details of transaction, such as the address of both sender and receiver and the amount to be transferred. The hash is uniquely created for each individual block to prove its identity and contents, serving as a fingerprint. When a new block is joint, the hash is calculated and any change that occurs inside the block after causes the hash to be changed, i.e. it is easy to detect changes when the hash is utilized. Therefore, any block that contains an invalid transaction will be discovered immediately and will not be admitted to the chain. Not only the block itself, but other blocks added later will also not be included in the chain [16], [17].

As shown in Figure 3, each of the continuously growing blocks has to refer to the previous block in the chain by including a cryptographic hash of the predecessor block, which forms a secure interconnection link between the blocks based on Public Key Infrastructure (PKI) encryption. This makes the blocks immutable and enables participants to trace information flows. However, the first block cannot point to and include the hash of previous block; and thus, it is considered as the parent of all new blocks and is referred to as the “Genesis Block” [18].

There are three types of Blockchain in terms of data management and availability: public or permissionless, private or persmissioned, and consortium. In public/permissionless Blockchain, the network access is widely open, and regardless of location, time, and operating conditions, any node can join and participate in the consensus process without any previous approval. It is almost impossible to tamper with the data in public Blockchain because the records are visible to all participants and the validation is distributed among a large number of nodes, i.e. the transactions are accessible to the public [16].

In contrast, in private/permissioned Blockchain, the network access is restricted, and any node that wishes to join and participate in the consensus process must obtain approval from the Blockchain owner. The records and validation of blocks in private Blockchain are fully centralized and managed by the owner; and therefore, data tampering could occur in this situaion. This type of Blockchain is suitable for enterprises seeking collaboration and sharing data while simultaneously requiring restricted access to their sensitive data [19].

Consortium Blockchain is a collaborative model mainly designed to bring together multiple enterprises that seek collaboration to improve business processes. The data is governed by a group of entities rather than a single individual as in private Blockchain and is not necessarily homogeneous across all blocks. The consensus process is determined by a selected set of nodes, which are managed via several organizations, including governments, supply chains, and central banks [16], [19], [20].

The main reason for the prominence of Blockchain among emerging technologies is that Blockchain technology is typically a public ledger completely open to anyone. In other words, it is a new approach of passing digital information between the users of Bitcoin, the most common cryptocurrency application, where the electronic cash is validated and securely transmitted between participants in a decentralized and peer-to-peer (P2P) manner [21]. Thus, all executed transactions must be approved and verified by all participating nodes, which creates irrefutable records to avoid data tampering and double-spending problems and ensure ledger consistency. Due to this unique feature, the majority of people who are involved in designing cybersecurity solutions recognize Blockchain as the best security solution capable of providing robustness and sustainability to any infrastructure [22], [23].

With Blockchain, each participating party is provided with a secure digital identity through holding two keys: a public key used for encryption and a private key used for decryption.

B. SOFTWARE DEFINED NETWORKING

Software Defined Networking (SDN) is an emerging technology adopted recently to ease and simplify network management and configuration, and it has gained tremendous momentum from industry and academia [24]. It is a relatively new way of building networks that promote a more robust environment by bringing dependability and security to the front of the process to prevent, detect, report, isolate, minimize, and possibly mitigate the harmful effects of most network intrusions. The essential concept that has boosted the innovation processes in the SDN technology is the centralization of the control plane, which is distributed with the data plane functionality inside the routers and switches in the traditional networks. In SDN, the control plane (network intelligence), which is responsible for making decisions on how to forward network packets, is typically removed from the part of the network, which is responsible for carrying and transmitting network traffic, i.e. the control plane is logically centralized in a software entity called an SDN controller. Through the SDN controller, network administrators can easily program and configure the all network elements directly from a single management point without the need to access each individual network device.

Figure 4 illustrates the conceptual architecture of SDN, which mainly includes three network layers: infrastructure layer, control layer, and application layer [25]. The infrastructure layer is a set of network devices with basic network functionality for handling and forwarding IP packets based on decisions given by the SDN controller, i.e. forwarding rules associated with actions initiated by applications running on the SDN controller and installed on network devices via the so-called southbound interface [26]. The next layer up is the control layer, where the logical and centralized SDN

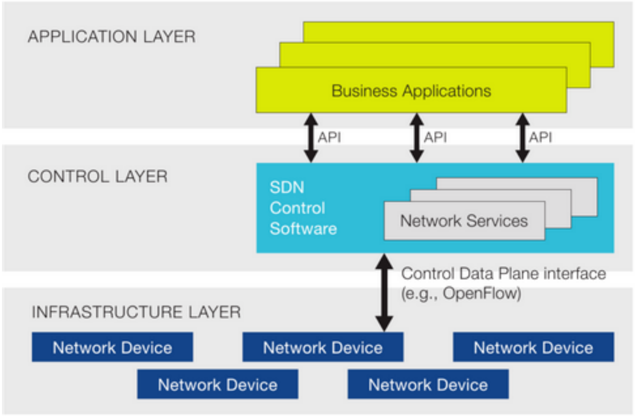

FIGURE 4. The architecture of software defined networks [25].

controller resides, which essentially acts as Network Operating System (NOS) that hides the complexity of underlying hardware and software infrastructure elements and provides a global view of the network to the application layer [27]. The application layer resides at the top of the SDN architecture, where network policies, such as Quality of Services (QoS), and security services, such as firewalling, are defined. The communication channel between the control and application layers is refereed to as the northbound interface, which currently has no well-established standard.

While SDN is more secure against some threats and provides scalable and extensible network monitoring tools, it presents new vulnerabilities that do not exist in traditional networks. In [15], the authors identified seven main threat vectors, such as forged or faked traffic flows, attacks on vulnerabilities in switches, control plane communications, and controllers, lack of trust mechanisms between controller and management applications and trusted resources for forensics and remediation that stand in the way of accomplishing a secure and robust network environment. Also, the aggregation of the entire network management and configuration in a centralized SDN controller is considered a single point of failure. Therefore, we believe that decentralizing some SDN security services and creating mutual trust between network entities without the need for a centralized entity, as in Blockchain, will significantly improve the robustness and enhance the security of the SDN architecture and guard its communication against a large proportion cyber incidents.

III. RESEARCH FINDINGS AND DISCUSSION

The topic of SDN and Blockchain have individually received immense attention from industry and academia. Even though both technologies have only existed for several years and are still in their infancy, to the best of our knowledge, this paper presents the first survey of previous efforts to apply Blockchain to the SDN architecture for the purpose of cybersecurity.

The expected contributions of our work are to answer the research questions shown in Table 1, and discuss the results based on observations obtained after reviewing the published papers. We carried out an in-depth analysis of security applications deployed in SDN using Blockchain technology and found out that most studies included in our paper proposed IoT solutions based on Blockchain to protect physical and intangible assets from tampering and data records from unauthorized access. Only a few studies have applied Blockchain technology to SDN for the purpose of security. For answering RQ1, we will briefly discuss the applications and their purposes, and for answering RQ2, we will demonstrate how these applications are implemented.

TABLE 1. Research questions.

Research Questions (RQs)	Discussion
RQ1: What are the latest SDN security applications implemented via Blockchain?	List cases where Blockchain was the core of providing a secure and resilient infrastructure to SDN. This will help understand the impact of Blockchain on the security of SDN.
RQ2: How does Blockchain provide and improve the security of SDN?	Discuss the characteristics of Blockchain that are mainly deployed to boost security in different SDN applications. This will help understand the implantation of Blockchain in SDN for security.

A. RQ1: WHAT ARE THE LATEST SDN SECURITY APPLICATIONS IMPLEMENTED VIA BLOCKCHAIN?

In [28], the authors address that the traditional architecture of cloud storage services cannot handle data flowing from IoT devices. The traditional architecture lacks in multiple aspects, including security, real-time data recovery, availability, and latency and cannot be scaled up easily. To improve the shortcomings of the traditional architecture, the authors propose a novel architecture based on Blockchain technology using a three-tier hierarchy cloud, fog layer, and IoT devices. It is cheaper and more secure and can provide real-time access to the data that emanates from IoT devices.

The paper [29] discusses the security issues of IoT, SDN, and the common security threats raised from using the SDN technology as the infrastructure for IoT nodes. The paper then proposes a novel architecture using Blockchain to combat most IoT security issues by mounting it on SDN infrastructure.

In the paper [30], the authors propose Blockchain technology to solve the problem of consensus and synchronization of multiple distributed SDN controllers used in Industrial Internet of Things (IIoT). Traditional approaches to get consensus from a distributed network lead to multiple issues, such as overhead, limited scope of network size, and liveliness properties. Thus, the authors propose a novel architecture utilizing SDN, Blockchain, and dueling deep Q-learning approach (DQL).

The paper [31] proposes a security framework using distributed Blockchain for vehicular IoTs in an SDN-enabled 5G vehicular ad-hoc network (VANET) environment. The key factor that drives this proposal is that in traditional vehicular IoT systems, a compromised vehicle can easily transmit incorrect data to the IoT cloud. Therefore, deploying

Blockchain technology is most likely the ideal approach to securing the vehicular IoT environment.

In [32], the authors propose a botnet prevention solution for IoT devices using SDN and Blockchain. The problem with the current infrastructure of IoT is that there is no policy in place to restrict the growing diversity of vendors, which could negatively affect the security and connectivity of IoT devices.

The paper [33] proposes DistBlockNet, a new architecture based on Blockchain technology mainly deployed in a distributed SDN to enhance the security, flexibility, and scalability of the IoT network. In the current implementation of the IoT network, it is difficult and sometimes impossible to detect attacks in real-time without imposing overheads on network resources.

A small number of published papers have discussed the current security problems with the SDN architecture and recommended the use of Blockchain applications to enhance the security and scalablity of SDN. The authors of [34] investigate the security challenges present in the SDN architecture and suggest that deploying Blockchain in SDN would build a mutual trust between multi-vendors and improve data standardization and fault resistance. There are no specific technical details provided in the paper, nor does it investigate the integration of Blockhain into the SDN architecture as we do in our paper.

In [35], the authors propose a novel architecture using Blockchain technology in the SDN environment with OpenStack as a cloud-based data center [36]. The aim of the research is to demonstrate how SDN, OpenStack, and Blockchain can be successfully merged to build a secure peer-to-peer communication among untrusted parties without interference from a third party verifier.

The paper [37] proposes an OpenFlow-based firewall that includes some SDN functionality to secure Blockchain nodes, which are vulnerable and can be compromised by adversaries, especially in a public Blockchain network. The goal of the paper is to secure Blockchain through SDN technology, in which network intelligence is being centralized.

In [38], the authors propose a defense mechanism that relies on SDN technology to protect a Blockchain network from a DNS amplification attack that targets the Blockchain nodes, halting their functionality and usability. The goal of the paper is to enhance the security of Blockchain nodes without adding extra load on network resources. The current implementations of Blockhain are not completely secure and the DNS amplification attack can be made against Blockchain nodes.

The paper [39] discusses the problem of propagation delay and its impact on data transmission. It proposes an SDN framework to optimize the efficiency of multipath data transmission in consortium Blockchain. The goal of the paper is to increase the utilization of common paths, which in current implementation can lead to sub-flow disorder and link saturation.

B. RQ2: HOW DOES BLOCKCHAIN PROVIDE AND IMPROVE THE SECURITY OF SDN?

Based on the preliminary analysis and investigation carried out on the implementation of Blockchain solutions mentioned earlier, we realized that Blockhain applications in SDN are capable of building a unforgeable and non-tamperable data structure. For instance, in [28], the proposed Blockchain-based distributed model consists of fog nodes that are SDN-enabled, a cloud, and devices, which play the role of monitoring public infrastructure environments before transforming filtered data to fog nodes. The fog nodes are made up of multiple fog computing entities deployed at the edge of the network to provide on demand access and cost effective, secure, and efficient computing infrastructure to IoT devices.

Each fog serves as a given community and provides localization, while the cloud layer implements smart contract-based Blockchain to provide network monitoring and ensure that there is security through detection of events and behavioral analysis. In this research, Blockchain technology is used as an authenticator to create an encrypted channel based on the public key cryptographic principle to verify the authenticity of tokens between members and deliver data securely from an edge device to the fog and cloud layers. A smart video surveillance network is placed at the edge fog devices, and each video frame sent by an untrusted fog node is tagged with a unique index to associate the smart contracts for recognizing a malicious threat.

The results published indicate that the proposed model improves the throughput and delay to identify attacks on an IoT network in real time. Therefore, if a flooding attack is launched on the architecture, Blockchain and SDN enable fog nodes to balance the load and minimize overheads. Compared to the traditional cloud-based IoT architecture, the proposed model dramatically lowers the utilization of computing resources, traffic load imposed on the core network, and delay in the communication channel between IoT devices.

In [29], the proposed architecture basically enables encrypted data transfer between two nodes irrespective of its network and geographical location. When SDN is deployed as a supporting network for IoTs, the security issues are increased ten-fold, due to the increase in the attack surface available for threats and severity of impact in case of compromise. For example, compromising an SDN controller, i.e. the central network intelligence system, has disastrous effects. SDN security issues can be discussed layer-wise as follows:

- The application layer is generally prone to unauthorized and unauthenticated access control due to the fact that the network access control in SDN is placed at a single and re-programmable entity. This implementation problem can be handled easily by multi-factor authentication.
- Improper rule insertion in the network disrupts some of the services, and debugging the installation of flow rules in the switches flow table to identify the source of the corruption is a mammoth task.

- A Denial of Service (DoS) attack can be launched against the control layer by generating multiple requests or malicious flows from a single or multiple nodes. To tackle this type of attack, a trusted-third party authenticator can be used; however, this is not suitable for a large environment when there are many IoT devices installed. The attack can be detected by observing the behavior of all nodes and applications through replication technique, which is capable of isolating and removing certain threats.
- In the data plane, the attacker can push rules into the SDN switches to create flooding attacks on the switches.
- Threats to the Transport Layer Security (TLS) of SDN can be utterly exposed as no authentication is required between SDN nodes prior to establishing connectivity.

Therefore, introducing IoTs in a highly volatile environment while there are many unresolved security issues leads to catastrophic results because the IoT devices have limited computation power and are deployed in areas that are difficult to access. Protection of unattended IoT devices must be ensured throughout their lifespan as developers often skip security requirements to prolong battery life.

Maintaining the trusted security status of devices is problematic because in a real life scenario monitoring all devices results in a constraint on network resources as well as interoperability issues between devices of different vendors. Thus, the authors suggested that all network traffic flowing between SDN and IoT devices should traverse a secure gateway node to ensure all the communication is authenticated via Blockchain technology.

In [30], permissioned Blockchain is used in distributed Software Defined Industrial Internet of Things (SDIIoT) to achieve a network-wide trusted and synchronized view and ensure reliability, safety, and traceability among distributed devices. Due to the constrained throughput of permissioned Blockchain, multiple other factors, such as the trust feature of Blockchain nodes and controllers as well as the computational power of the architecture are utilized to improve and enhance network throughput. Further, they identified view changes, including access selection and computational resources, as an optimization issue.

The key reason for implementing a protocol that uses permissioned Blockchain-based consensus among distributed SDN controllers is to achieve simplicity and security during the collection phase and network synchronization. Each controller gathers the OpenFlow commands and local events that are digitally signed with Message Authentication Code (MAC) to ensure the integrity and authentication of the transactions; it then issues consensus to a third party Blockchain system. One controller is selected to verify the access of the validated and unvalidated blocks and then forwards those blocks to the remaining controllers. In this way, network-wide controllers are synchronized.

By theoretical analysis, the authors calculate the cost of MAC generation per transaction and its maximum effect on the throughput, which is improved through a Markov decision process [40]. The simulation results are compared among different proposed schemes and the existing traditional scheme. The results show a massive change in behavior after applying the dueling deep Q-learning (DQL) approach.

The authors of [31] enforce a traffic condition tag on vehicles, which contains current road information, and broadcast the information in the tag to all other vehicles in the network. The aim is to prevent a compromised vehicle from injecting incorrect traffic-related data in real time to its neighboring vehicles, which will score the tag. Road Side Units (RSUs) are a data scheduling scheme in vehicular IoT services used to ensure timely broadcast of information required by stakeholders. It is implemented such that an RSU receives the tag information and evaluation from neighboring vehicles, and based on the distance between vehicles, the RSU calculates the trust value for the broadcasting vehicle and stores it in a block for future reference.

The proposed system holds elections in regular intervals based on Blockchain technology, i.e. proof of work (PoW) and proof of stake (PoS). The system essentially identifies compromised vehicles based on accurate information distributed via the vehicles. As a consequence, the compromised vehicles are temporarily banned from pushing updates to the vehicular IoT environment. This ensure the privacy and anonymity of the legitimate vehicles. In the scheme, the user identity is not available to the operator or vehicles, as information about user's identity and vehicle authentication is typically excluded and stored separately to protect the user's privacy.

The architecture of the proposed framework mainly includes a centralized authentication system, partially centralized road conditions, traffic live-streaming videos, and a distributed Blockchain-based trust management system. The heterogeneous nodes that consist of RSUs, 5G base stations (gNBs), and on-board units (OBUs) are installed on the vehicle. The tasks carried out by Blockchain technology are vehicle registration, road condition information, and message sharing service. The authors conduct a detailed theoretical and numerical analysis followed by safety analysis of the proposed architecture. The published results depict of the system is accurate and effective. The significant improvement here is that the process of encrypting a high quality video creates an acceptable overhead on the system. The threats against the proposed system are user privacy, compromised vehicle, forged scoring, and compromised RSU. The first three issues are addressed by Blockchain technology, while the deployment of multiple RSUs and miner election at a regular interval ensure that a compromised RSU is detected because it is impossible for an attacker to infiltrate multiple RSUs at the same time.

The paper [32] addresses that IoT devices are rapidly increasing in number, which simultaneously leads to issues of connectivity, security, management, and chance of being part of a botnet to launch a Distributed Denial of Service (DDoS) attack. According to the researchers, the Internet of

Everything (IoE) is leading to more and new issues rather than resolving current ones, and thus they recommended new strategies that require the number and type of IoT manufacturers to be limited. The strategies also enforce a strong policy on IoT devices, which specifies the minimum security requirements and the time and duration of scheduled network scans that runs automatically at a specific frequency. Moreover, network segmentation is recommend for those who are seeking a better network management, irrespective of the computational overhead on network resources.

The proposed scheme integrates an SDN controller with Blockchain to efficiently handle the distributed nature of IoT devices, which is considered a challenge when new security mechanisms are applied. The scheme is automated and does not require manual intervention from network administrators. The network view consists of three modules: Security Policy Module (SecPoliMod), Controller Module (ConMod), and Log Module (LogMod), where SecPoliMod and ConMod are essentially designed to prevent IoT devices from being used as botnets, while LogMod monitors network traffic destined to the devices to ensure their legitimacy. SecPoliMod relies on the colored coins concept introduced by Blockchain technology to enforce security policy and distinguish between legitimate and illegitimate connected devices. If a device is colored, it means the device has met the minimum security requirements for connecting to the network. However, if no label is defined on the device, network traffic flowing from that device will be isolated and dropped by the switches before merging with other network traffic.

The authors of [33] propose a new scheme called DistBlockNet, which utilizes some Blockchain features to provide a trusted peer-to-peer network among non-trusted members without a third party verifier. In DistBlockNet, all controllers are interconnected with each other to facilitate communication between IoT forwarding devices because each view of the network includes three modules: Shelter module, OrchApp module, and Controller. The Shelter and OrchApp modules are mainly designed to work in parallel to provide security for the IoT network-based SDN infrastructure. The former module is used as an application-control layer, and the latter one is used as a control-data layer. The Shelter module is also used to gather information about the network architecture. In general, DistBlockNet provides incident prevention from repetitive threat attacks without any manual inputs or decisions. The architecture includes a controller (verifier) node used to both update and manage the flow rules in the table and a request/response node used only to update the flow rules. The authors observed the CPU usage when the proposed system is under flooding attack and found that DistBlockNet is capable of serving many IoT devices with minimal increase in overhead.

The authors of [35] propose a new architecture to secure SDN from common threats by deploying Blockchain technology. This would provide security and authentication between different SDN entities without the need for a centralized controller because security is the biggest concern for the stakeholders. The deployed solution is referred to as Blockchain security over SDN (BSS), which protects the privacy and availability of SDN elements involved in the file sharing process from being captured and seen by untrusted entities. For the experiment, the authors use Mininet emulator for a programmable SDN topology, OpenStack as cloud data storage, and OpenDaylight controller for integration [41], [42]. For testing, they used Blockchain contracts, created via the Serpent programming language, Ethereum platform, and Pyethereum tester tool [43]. To ensure robustness of transaction, the Blockchain file is encrypted using SHA-256 and Pyethereum, and then inserted in SDN via Serpent. The performance of the approach is evaluated on the basis of file accessibility to trusted and non-trusted members, and the reliability of the entire SDN environment is evaluated before and after authentication takes place through BSS, which later proves that the proposed mechanism is able to provide security to the SDN architecture.

In [37], ChainGuard is proposed as a new SDN module applied to the Blockchain architecture to protect nodes participating in the chain. In this implementation, network traffic must pass through a ChainGuard-enabled controller to further investigate network traffic and monitor overall behavior. When the controller recognizes abnormal behavior flowing between the Blockchain nodes, it immediately blocks the attacking node, i.e. the source of the malicious traffic. In this case, ChainGuard ensures that the attack is quarantined for further investigation and does not affect the whole infrastructure. The deployment of ChainGuard mechanisms is relatively simple and cheap since there are no changes or updates required to the Blockchain software.

There are three labels to describe the status of Blockchain nodes: legitimate, illegitimate, and not yet considered. All nodes are itemized into one of the three lists maintained at the controller, i.e. whitelist, graylist, and blacklist, respectively. With the ChainGuard controller, access is maintained by keeping nodes in their specific category and tracking illegitimate nodes as well. To prevent a flooding attack, ChainGuard relies on the greylist and limits the number of tokens. These techniques are based on using a limited number of flow entries and dropping the remainder. Experiments were conducted by flooding the network with DoS and DDoS attacks, and the results show that the Blockchain nodes under attack function properly and traffic flows remain undisrupted.

The authors of [38] propose ChainSecure, a proactive solution that essentially prevents Blockchain applications and nodes from a typical DNS amplification attack. The solution is based on the functionality of SDN and is deployed in a private Blockchain. OpenFlow switches are also utilized in this solution to create an innovative stateful mapping scheme (SMS) that facilities the discovery of potential attacks and security flaws. In the OpenFlow switches, DNS request packets are filtered based on their header fields and compared with corresponding response packets. If there is no match between the fields in the DNS request and response packets, the switch involved in the process will drop the illegitimate traffic before

TABLE 2. Critical analysis of recent studies.

Purposed Solution	Reason for Proposal	Critical Analysis	Technique used
A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT [28].	The current cloud architecture technology is unable to satisfy the future requirements of a scalable IoT network.	A distributed cloud architecture is proposed using three evolving technologies: SDN, fog computing, and Blockchain. With the use of Blockchain and SDN technology, the authors provide a programmable interface to the network and ensure scalability, high availability, adaptability, reliability, and secure services. In the architecture cloud and fog nodes are used for processing data, and Blockchain is used to ensure the integrity of the transmitting data. Nevertheless, the data stored at the server end is in unencrypted form, which raises the threat of leakage of sensitive data, compromising data confidentiality. In this approach, the fog nodes provide secure data delivery services between the cloud and IoT devices. The Blockchain functionality is being utilized to achieve cost effective access control service.	Blockchain, SDN, IoT.
Enhancing SDN security for IoT-related deployments through Blockchain [29].	The current communication channel between IoT devices in SND is unencrypted.	A comprehensive study on the security issues of SDN and IoT devices is conducted to highlight how both evolving technologies compliment and hinder the functionality of each other. Blockchain technology is the solution provided to resolve the security issues in SDN and IoT and provide data encryption.	Blockchain, SDN, IoT.
Blockchain-Based Software-Defined Industrial Internet of Things: A Dueling Deep Q-Learning Approach [30].	The current network architecture of SDI-IoT is not synchronized.	Permissioned Blockchain-based consensus protocol with Dueling DQL is able to ensure synchronization in trusted networks and improves throughput via offloading computing tasks to computer resources hosted at the edge servers, resulting in maximizing the optimization. The deployment of permissioned Blockchain would definitely reduce the building blocks of network performance, i.e. cost, latency, and bandwidth utilization, while MAC would ensure integrity and authentication of transactions.	Blockchain, SDN, IIoT.
Blockchain-Based Secure and TrustworthyInternet of Things in SDN-Enabled 5G-VANETs [31].	The current vehicular IoT environment is insecure since a compromised vehicle can go undetected and spread incorrect road information.	The Distributed Blockchain-based security framework is capable of securing vehicular IoT services in an SDN-enabled 5G VANET. Blockchain technology is used to secure the tags that include traffic updates and live video clips and provide verification upon request. Blockchain is used to keep record of information generated by the vehicles and video clips are encrypted and sent to the cloud in case the proof is required later. The real-time service feature is also incorporated in the system to weed out compromised vehicles and RSUs. The trusted management system is designed based on Blockchain technology to identify compromised nodes and verify legitimate vehicles, i.e. no forged or fake tags are accepted.	Blockhain, SDN, IoT, 5G, VANET.
DDoS Botnet Prevention using Blockchain in Software Defined Internet of Things [32].	The current infrastructure of IoT is insecure and does not prevent IoT devices from being used as bonets.	Integrating Blockchain technology into SDN is capable to prevent IoT devices from being used as botnets that launch DDoS attacks. The colored coin concept from Blockchain is used to differentiate between IoT devices that meet the minimum security requirements from the ones that do not meet the security requirements, which will be transferred for further processing. The proposed solution has been implemented on an emulation environment and the results has been evaluated and analyzed to verify the efficiency and effectiveness of the solution.	Blockhain, SDN, IoT.
DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks [33].	The current infrastructure of IoT lacks in terms of scalablity and flexibility when there is no centralized authenticator.	Blockchain and SDN together can provide a secure, flexible, and scalable framework for IoT without the need for a trusted third party. Blockchain technology is used to ensure the flow rules in the table that are updated automatically according to the threat landscape, i.e. it does not require manual input.	Blockhain, SDN, IoT.
Research on Key Technologies of Software-Defined Network Based on Blockchain [34].	The current SDN architecture is insecure and vulnerable.	Merging Blockchain technology with SDN would mitigate most security problems exist in SDN.	Blockchain, SDN.
Blockchain Security over Software Defined Network [35].	The current SDN architecture is insecure and vulnerable and lacks data privacy, authentication, and availability.	Integrating Blockchain technology and OpenStack into the SDN environment is a promising solution to ensure security and reliability. With this in place, files are transmitted securely among SDN hosts. The smart contracts can also be used to ensure transparency and security and allow the concerned party to track licensing, delivering, complaints, etc. The Blockchain functionality utilized ensures cost effectiveness and reliability. The experiments conducted in this paper ensure that Blockchain can be used to secure an SDN environment integrated with OpenStack	Blockchain, SDN, OpenStack.
ChainGuard - A Firewall for Blockchain Applications using SDN with OpenFlow [37].	Blockchain nodes are insecure, especially in the public Blockchain network.	The nodes participating in a public Blockchain network are secured only when the OpenFlow-based Firewall is applied. The security framework, ChainGuard, which includes the SDN functionality is able to efficiently filter network traffic and distinguish between normal and malicious. The module does not require any changes, updates, or upgrades of the Blockchain software.	Blockchain, SDN

TABLE 2. *(Continued.)* Critical analysis of recent studies.

ChainSecure - A Scalable and Proactive Solution for protecting Blockchain applications using SDN [38].	Blockchain nodes are vulnerable to DNS amplification attack in the private Blockchain.	A defensive mechanism that uses Stateful Mapping Scheme (SMS), Entropy Calculation Scheme (ECS), and SDN technology can protect Blockchain nodes from DNS amplification attack. The proposed model, ChainSecure can combat the DNS amplification attack with only minimum effect on network performance, where most existing solutions require more resources for the computation process, which certainly overloads the control plane and exhausts the TCAM memory. The performance evaluation conducted in the research indicates that ChainSecure can effectively defend against the DNS amplification attack with low overhead on the network resources. The proposed mitigation solution is feasible in the private Blockchain i.e. restricted number of nodes, and has not considered the public Blockchain.	Blockchain, SDN, ECS, SMS
SDN-based Optimizing Solutions for Multipath Data Transmission Supporting Consortium Blockchains [39].	The current implementation of the consortium Blockchain does not have a module that is efficiently capable of handling a group of sub-flows together	The multipath data transmission technique based on the SDN functionality can be applied in consortium Blockchain to have optimal path selection features. It also makes the network infrastructure more flexible and scalable through dividing network traffic to sub-flows that minimizes propagation delays.	Blockchain, SDN

hitting the SDN controller. Normally, OpenFlow switches use Ternary Content Addressable Memory (TCAM) for this purpose, which can easily be flooded due to its limited size. In the proposed solution, a robust detection mechanism based on the Entropy Calculation Scheme (ECS) is implemented via sFlow to run on top of the SDN controller, mainly to protect the Blockchain nodes without requiring modifications to the Blockchain software. ECS is fundamentally an information theory concept that evaluates the ambiguity of incoming data. To prove the efficiency of ECS, the authors measure detection rate and quantify errors associated with data reporting.

In [39], a novel SDN-based framework that relies on multipath data transmission is proposed to improve the propagation delay problem and bandwidth on the common link of paths. Multipath data transmission is an efficient mechanism to transfer data and resolve the traffic congestion caused when receiving information from a dedicated server, especially in consortium Blockchain, i.e. semi-private Blockchain with multiple controlling entities. Traffic congestion occurs when data is transferred through multiple overlapping links, and data thus encounters various levels of propagation delay, creating flow disorders at the receiver end. The proposed solution mitigates the traffic congestion issue by increasing the bandwidth, which is shared among the members, and using SDN, which provides a centralized controller capable of defining sub-flows and ensure nominal propagation delays and link overlapping. The authors take advantage of one of the main features of SDN, topology discovery, to maintain flows and selection of the shortest path. Topology discovery is generally used to map the social network organized by consortium Blockchain and evaluate the most efficient route to get the data. The evaluation conducted in this research shows that when the data-sampling rate is higher than 100%, sub-flow accuracy is achieved. For path selection, the authors propose a novel algorithm that ensures minimal propagation delay and improves throughput, which was 50% higher than in traditional multipath data transmission.

Table 2 summarizes the papers discussed in this research.

IV. FUTURE CHALLENGES AND DIRECTIONS

The inherent separation between the control and data planes inherently in SDN brings new approaches to performing well-known attacks in different manners. For example, a DDoS attack can target the control plane to saturate the SDN controller and make it unresponsive. This is a serious threat to the SDN architecture, which ultimately brings the entire service down. Attacks must be identified and efficiently mitigated before reaching the network. Therefore, merging Blockchain technology with SDN seems to be a promising and effective solution that achieves cyber-secure network architecture. We can take advantage of the decentralization aspect, introduced in Blockchain and distribute some of the network functionalities without the need for additional security hardware devices.

The following SDN components are insecure and vulnerable to different attack vectors, as discussed in other papers:

- Topology discovery, which provides the SDN controller with the network graph, is vulnerable to the Link Fabrication attack, where the attacker can easily inject a spoofed LLDP packet to poison the entire view of the network [44]. We can apply Blockchain and distribute the authentication of the LLDP packets among the network devices to ensure no spoofed packets are allowed.
- Address Resolution Protocol (ARP) is the protocol that maps the network addresses to the corresponding hardware addresses (MAC) and populates the ARP cache. According to [45], the current implementation of this protocol in SDN is insecure and vulnerable to ARP attack, where the attacker can easily poison the ARP

cache with false information to launch DoS or MITM attacks. We can apply Blockchain and distribute the authentication of ARP packets among SDN hosts instead of centralizing the process.

- SDN virtualization, which allows multiple SDN controllers to run simultaneously over the same network infrastructure, is vulnerable to multiple attacks, as discussed in [46]. We can apply Blockchain and distribute the authentication of the network packets traversing through the SDN virtualization.

Due to the scope of this review paper, we will leave the implementation details for our future work. We will revisit these components and investigate security vulnerabilities to purpose persistent solutions that take advantage of Blockchain technology.

V. CONCLUSION

Software Defined Networking (SDN) breaks the vertical integration of the data and control planes, and moves the network's control logic to a centralized entity called an SDN controller. Although, this implementation improves network management and configuration, the SDN architecture is still vulnerable to a multitude of cyber attack types.

Blockchain technology is the opposite of SDN, in which data is decentralized and eliminates the need for a trusted third party in a P2P network. Blockchain is categorized as public, private, or consortium based on the accessibility of transactions. In public Blockchain, all nodes take part in the consensus procedure and view the transaction details. However, in private and consortium Blockchain, accessibility of transactions is granted and revoked based on a decision made by a centralized entity, and only limited numbers of preapproved nodes take part in the consensus procedure.

This paper discussed previous works that have merged Blockchain technology with SDN to design solid cybersecurity solutions for protecting the SDN architecture from attacks. Although research efforts have made excellent progress towards securing SDN, an intrusion detection and threat mitigation mechanism that can protect the control and data planes and communication channel has yet to developed. Thus, this paper also offered a strategic vision for utilizing Blockchain technology and taking advantage of its features to ensure security of SDN and create an opportunity for more scalable and efficient SDN architecture.

ACKNOWLEDGMENT

The author would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project R-1441-58.

REFERENCES

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Manubot, Tech. Rep., 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf

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

[3] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the Bitcoin economy," *Pitt. Tax Rev.*, vol. 12, p. 25, Apr. 2014.

[4] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of Bitcoin," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw.*, 2015, pp. 184–191.

[5] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[6] *Size of the Blockchain Technology Market Worldwide*. Accessed: Aug. 19, 2019. [Online]. Available: https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/

[7] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 464–467.

[8] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2016, pp. 1–3.

[9] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun. IEEE 14th Int. Conf. Smart City; IEEE 2nd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2016, pp. 1392–1393.

[10] H. Kakavand, N. Kost De Sevres, and B. Chilton, "The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies," in *Bart, The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*. Rochester, NY, USA: SSRN, Jan. 2017.

[11] J.-H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry [future directions]," *IEEE Consum. Electron. Mag.*, vol. 6, no. 3, pp. 19–23, Jul. 2017.

[12] H. Halaburda, "Blockchain revolution without the blockchain," Bank Canada Staff Anal. Note, Canada, Appl. Note 5, 2018.

[13] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tutr.*, vol. 15, no. 4, pp. 2046–2069, 1st quart,. 2013.

[14] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proc. USENIX Conf. Usenix Annu. Tech. Conf.*, 2016, pp. 181–194.

[15] D. Kreutz, F. M. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, 2013, pp. 55–60.

[16] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data*, Jun. 2017, pp. 557–564.

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

[18] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in *Proc. 2nd Int. Conf. Contemp. Comput. Inform. (IC3I)*, Dec. 2016, pp. 463–467.

[19] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[20] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.

[21] *Cryptocurrencies by Market Capitalization*. Accessed: Aug. 19, 2019. [Online]. Available: https://www.coinmarketcap.com/

[22] D. Schutzer, "CTO corner: What is a Blockchain and why is it important? FSRoundtable," FS Roundtable, Washington, DC, USA, Tech. Rep. 16, 2016.

[23] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.

[24] N. McKeown, "Software-defined networking," *INFOCOM Keynote Talk*, vol. 17, no. 2, pp. 30–32, 2009.

[25] Open Networking Foundation, "Software-defined networking: The new norm for networks," ONF, Menlo Park, CA, USA, White Paper 2, 2012, pp. 2–6.

[26] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, 2008.

[27] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, S. Shenker, "NOX: Towards an operating system for networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 3, pp. 105–110, 2008.

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

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

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

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

[32] Q. Shafi and A. Basit, "DDoS Botnet prevention using blockchain in software defined Internet of Things," in *Proc. 16th Int. Bhurban Conf. Appl. Sci. Technol.(IBCAST)*, Jan. 2019, pp. 624–628.

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

[34] C. Xue, N. Xu, and Y. Bo, "Research on key technologies of software-defined network based on blockchain," in *Proc. IEEE Int. Conf. Service-Oriented Syst. Eng. (SOSE)*, Apr. 2019, pp. 239–2394.

[35] S. R. Basnet and S. Shakya, "BSS: Blockchain security over software defined network," in *Proc. Int. Conf. Comput., Commun. Automat. (ICCCA)*, May 2017, pp. 720–725.

[36] O. Sefraoui, M. Aissaoui, and M. Eleuldj, "OpenStack: Toward an open-source Solution for Cloud Computing," *Int. J. Comput. Appl.*, vol. 55, no. 3, pp. 38–42, Oct. 2012.

[37] M. Steichen, S. Hommes, and R. State, "ChainGuard—A firewall for blockchain applications using SDN with OpenFlow," in *Proc. Princ., Syst. Appl. IP Telecommun. (IPTComm)*, Sep. 2017, pp. 1–8.

[38] Z. A. El Houda, L. Khoukhi, and A. Hafid, "ChainSecure-a scalable and proactive solution for protecting blockchain applications using SDN," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[39] W. Hou, Z. Ning, L. Guo, and P. Guo, "SDN-based Optimizing solutions for multipath data transmission supporting consortium blockchains," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Jul. 2018, pp. 1–5.

[40] M. L. Puterman, *Markov Decision Processes.: Discrete Stochastic Dynamic Programming*. Hoboken, NJ, USA: Wiley, 2014.

[41] R. L. S. De Oliveira, C. M. Schweitzer, A. A. Shinoda, and L. R. Prete, "Using mininet for emulation and prototyping software-defined networks," in *Proc. IEEE Colombian Conf. Commun. Comput. (COLCOM)*, Jun. 2014, pp. 1–6.

[42] J. Medved, R. Varga, A. Tkacik, and K. Gray, "Opendaylight: Towards a model-driven SDN controller architecture," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2014, pp. 1–6.

[43] R. Anderson, E. Biham, and L. Knudsen, "Serpent and smartcards," in *Proc. Int. Conf. Smart Card Res. Adv. Appl.* Berlin, Germany: Springer, 1998, pp. 246–253.

[44] T. Alharbi, M. Portmann, and F. Pakzad, "The (in)security of topology discovery in software defined networks," in *Proc. IEEE 40th Conf. Local Comput. Netw. (LCN)*, Oct. 2015, pp. 502–505.

[45] T. Alharbi, D. Durando, F. Pakzad, and M. Portmann, "Securing ARP in software defined networks," in *Proc. IEEE 41st Conf. Local Comput. Netw. (LCN)*, Nov. 2016, pp. 523–526.

[46] T. Alharbi and M. Portmann, "The (in)security of virtualization in software defined networks," *IEEE Access*, vol. 7, pp. 66584–66594, 2019.

TALAL ALHARBI received the master's degree in network security and system administration from the Rochester Institute of Technology (RIT), Rochester, NY, USA, and the Ph.D. degree in security of software defined networks from The University of Queensland (UQ), Brisbane, QLD, Australia. He was the Vice Dean of Systems and E-services, IT Deanship. He is currently an Assistant Professor and the Vice Dean of Academic Affairs, College of Computer and Information Sciences, Majmaah University, Al Majma'ah, Saudi Arabia. His research interests include computer networks, networks security, software defined networks, cyber security, and blockchain technology. He also obtained two advanced certificates from RIT focused on network planning and design and information assurance.