symmetry

MDPI

Review

Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight

Sharyar Wani [1,*], Mohammed Imthiyas [2], Hamad Almohamedh [3,*], Khalid M Alhamed [4], Sultan Almotairi [5,*] and Yonis Gulzar [6]

1 Department of Computer Science, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia
2 Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia; imthiyasm811@gmail.com
3 Faculty of King Abdulaziz City for Science and Technology (KACST), Riyadh 12354, Saudi Arabia
4 IT Programs Center, Faculty of IT Department, Institute of Public Administration, Riyadh 11141, Saudi Arabia; hamedk@ipa.edu.sa
5 Department of Natural and Applied Sciences, Faculty of Community College, Majmaah University, Majmaah 11952, Saudi Arabia
6 Department of Management Information Systems, College of Business Administration, King Faisal University, Al-Ahsa 31982, Saudi Arabia; ygulzar@kfu.edu.sa
* Correspondence: sharyarwani@iium.edu.my (S.W.); halmohamedh@kacst.edu.sa (H.A.); almotairi@mu.edu.sa (S.A.)

Abstract: Distributed Denial of Service (DDoS) attack is a major threat impeding service to legitimate requests on any network. Although the first DDoS attack was reported in 1996, the complexity and sophistication of these attacks has been ever increasing. A 2 TBps attack was reported in mid-August 2020 directed towards critical infrastructure, such as finance, amidst the COVID-19 pandemic. It is estimated that these attacks will double, reaching over 15 million, in the next 2 years. A number of mitigation schemes have been designed and developed since its inception but the increasing complexity demands advanced solutions based on emerging technologies. Blockchain has emerged as a promising and viable technology for DDoS mitigation. The inherent and fundamental characteristics of blockchain such as decentralization, internal and external trustless attitude, immutability, integrity, anonymity and verifiability have proven to be strong candidates, in tackling this deadly cyber threat. This survey discusses different approaches for DDoS mitigation using blockchain in varied domains to date. The paper aims at providing a comprehensive review, highlighting all necessary details, strengths, challenges and limitations of different approaches. It is intended to serve as a single platform to understand the mechanics of current approaches to enhance research and development in the DDoS mitigation domain.

Keywords: distributed denial of service (DDoS); DDoS attack; DDoS mitigation; DDoS defense; blockchain

Citation: Wani, S.; Imthiyas, M.; Almohamedh, H.; Alhamed, K.M; Almotairi, S.; Gulzar, Y. Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight. *Symmetry* **2021**, *13*, 227. https://doi.org/10.3390/sym13020227

Academic Editor: Christos Volos
Received: 8 December 2020
Accepted: 26 January 2021
Published: 29 January 2021

1. Introduction

A distributed denial of service (DDoS) attack is a special type of denial of service attack that overwhelms the target or the related infrastructure with malicious traffic. This is achieved using bots, a network of malware compromised computers and other devices, under the remote control of an attacker (refer to illustration in Figure 1) [1]. It severely hampers the bandwidth and connectivity leading to disruption of all services on the network [2]. Cloud ecosystems suffer maximum loses due to complete service denial and service degradation [3]. The primary target of DDoS attack is availability of resources for genuine users. The malicious flooding overloads the network, exceeding its bandwidth capabilities and disrupting the services [4]. The target range varies from financial institutions, health care providers and government agencies to low key public networks [2].

It is difficult to distinguish the attack traffic in a DDoS attack because of its similarity to the legitimate traffic [5]. They behave very closely to normal network packets, albeit in higher quantities and concentration towards the victim [6]. This is more prevalent during the early stages of attack, especially in low-rate and low-traffic attacks [5]. The attack is usually measured in volumetric parameters such as packets-per-second, bits-per-second and connections-per-second [6]. A malicious attack from a small number of nodes is easier to detect and mitigate. DDoS uses a significantly large number of nodes, and the collective behavior drastically severs any chance of serving non-malicious requests [7]. The compromised devices transfer a large volume of packets without any breaks over the network, tricking the victim into recognizing them as legitimate traffic. As a result, not only does the host communicate with different devices but with different types of packets as well [8]. DDoS attack has been proven as a resource battleground between the defenders and attackers; the more the resources, the higher the chance of success [9].

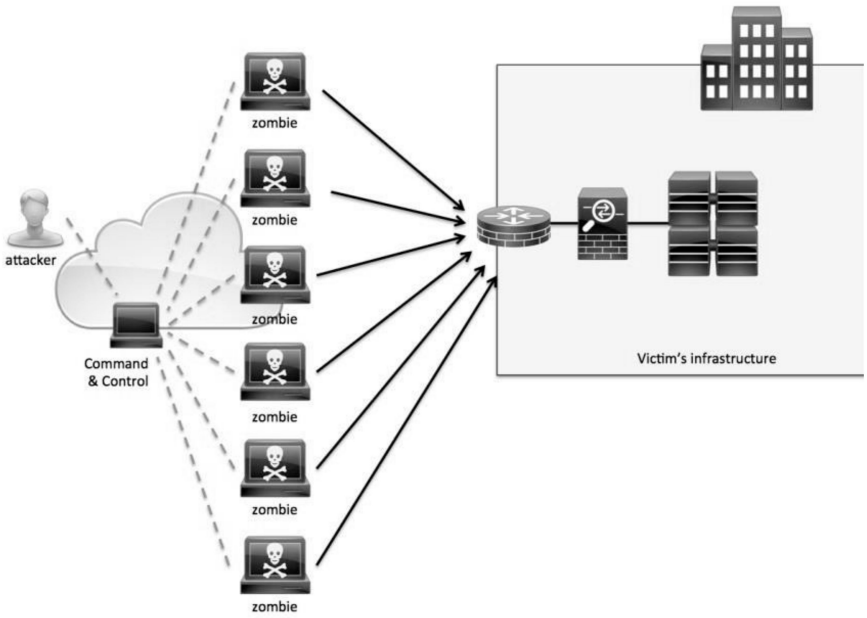

Figure 1. Distributed denial of service (DDoS) attack [6].

DDoS attacks can be classified as brute-force attacks, spoofing attacks and flooding attacks. Flooding attacks are the most common and severe among the three, thwarting the network bandwidth and blocking all legitimate requests. Survival approaches are focused on single target victims and require victims to detect and manage the attack themselves. However, a network wide flood requires mitigation approaches before it reaches the victims, making it suitable for multi-targeted attack. DDoS cannot be blocked or prevented altogether by installing software patches and deploying appliances. Therefore, Internet service providers either use scrubbing services or over provision their networks. Both the methods are financially not feasible [10].

The DDoS architecture consists mainly of zombies based on handlers' models and Internet relay-chat. All communications between the handler and the attack are usually encrypted, making the attack invisible from detection. Attackers spoof MAC and IP addresses and are geographically well distributed, making detection a tedious effort.

DDoS attacks have rapidly evolved over time and have become very sophisticated. DDoS attacks severely affect an organization's computing, financial and infrastructural resources [11]. The number of DDoS attacks has increased exponentially over the years, not even sparing major cloud service providers such as Microsoft and Amazon EC2 [5]. Around 79 countries were affected by DDoS attacks during the first quarter of 2018. The longest attack duration was about 297 h [12]. A 1.3 TBps attack was reported affecting GitHub. A 1.7 TBps attack was reported later following the attack on GitHub [13]. Some

established banks were severely affected by a peak 160 Gbps and 32 million packets per second DDoS attack in April 2019 [14]. Monetary losses of about $491 billion were reported in 2014 alone [11]. Amidst the COVID-19 pandemic (mid-August 2020), a world-wide DDoS extortion attack amounting to 2TBps, targeting finance and the travel industry, was reported by NetScout [15]. It is predicted that DDoS attacks will double from 7.9 million in 2018 to 15.4 million by 2023 [16]. These numbers, attack traffic and timings clearly indicate the threat severity of DDoS attacks [14].

Different methods and technologies have been employed in previous years to tackle this severe resource drainer attack, such as machine learning [17–19], deep learning [20,21], reinforcement learning [22], SDN [23–27], protocol tuning [28,29], network traffic classifiers [30,31], network function virtualization [32–34], fog computing [35] and reputation scoring, among others. In addition to struggling with scalability, high computation and communication overhead, the aforementioned methods do not perform effectively in real world DDoS attacks. They not only suffer because of increased volume of botnet and amount of traffic involved [13,15] but also due to the ever-increasing sophistication and complexities of DDoS attacks [11].

1.1. Problem Statement

Given the limitations and current state of the aforementioned approaches and ever-increasing erudition of DDoS attacks, there is a demand and need for more efficient solutions based on new technologies for detection and mitigation. In this context, blockchain has emerged as a promising partner, leveraging its fundamental characteristics of decentralization, internal and external trustless attitude, immutability, integrity, anonymity and verifiability to tackle DDoS attacks.

1.2. Motivation

It is necessary to have a holistic understanding about the application of new technologies in order to enhance the efficiency. Therefore, it is important to conduct a comprehensive survey about DDoS mitigation using blockchain technology. To the best of our knowledge, there does not exist a single survey discussing advancements specifically related to DDoS mitigation employing blockchain. Either the surveys focus on other DDoS mitigation technologies and techniques or include some of the blockchain-based studies for a particular domain as a part of their review. Therefore, this review aims to cover this knowledge gap in order for this domain to research novel and effective solutions using blockchain.

1.3. Objectives/Contributions

Following the discussion, this paper mainly intends to achieve the following objectives:

1. To discuss current applications of blockchain for DDoS mitigation in all related domains
2. To provide a comprehensive review of researches surrounding this domain
3. To classify mitigation approaches based on the dominant method/technology/technique
4. To tabulate essential findings of all related papers, providing a quick insight about the progress in this field of study

1.4. Paper Organization

The remainder of the paper is structured as follows: Section 2 lays the foundation of the domain knowledge by discussing key concepts in DDoS attacks and blockchain. Section 3 details the process of this review, including inclusion and exclusion criteria. Section 4 presents the in-depth comprehensive review of the extracted relevant studies in this domain. Finally, Section 5 highlights limitations and opportunities, while Section 6 concludes the study, highlighting the need to pursue the domain of the current study.

2. Theoretical Background

2.1. DDoS Attack Types

DDoS attacks are aimed at denying service access to legitimate users targeting availability of network resources. The attack procedure relies heavily upon distributed access to devices exploiting known vulnerabilities [36]. Attacks are targeted at various layers of the network infrastructure, e.g., application layer, transport layer, etc. [37,38]. Based on the network architecture, DDoS attacks are classified as follows [39]:

1. Application layer attacks: This is a layer seven network architecture attack aimed at target resource exhaustion leading to denial of service [38]. The attacker leverages application or system vulnerabilities, causing network instability. These attacks are often mistaken as implementation errors because of the low rate traffic required to execute them successfully. Examples include HTTP flood, Slowloris and Zero-day attack. An HTTP flood is an attack whereby continuous access is requested from multiple devices, exhausting the capabilities of the targeted device. A typical setup for an HTTP flood is presented in Figure 2. Slowloris sends incomplete requests at predefined intervals, aiming at keeping the request channels engaged for an extended period of time, preventing legitimate access to the target devices [37–41].
2. Resource exhaustion attack: Network layer and transport layer vulnerabilities are exploited by this DDoS attack. These are also referred as state exhaustion attacks depleting computing resources such as computational power and primary and secondary memories. Since this attack exploits protocol vulnerabilities in addition to being voluminous, it forms a hybrid between specific messages and volume being sent to the victim. TCP SYN floods send SYN messages to the victim but provide no confirmation to the victim for establishment of a connection with spoofed source IP addresses. In this manner, the target resources are exhausted over time, since it responds to each hand shake but never receives any confirmation from the attacker [37,41]. Other examples include Ping of Death, which are ping packets greater than 65,535 bytes, making the victim inaccessible, and Smurf attack, which destabilizes the victim services by sending a large volume of ICMP packets [39,41]. As seen in Figure 4, the attacker creates a network packet attached to a false IP address (spoofing), transmitting an ICMP ping message. The network nodes are required to reply. The replies follow an infinite loop by being sent back to the network IPs.
3. Volumetric attacks: Massive amounts of data are sent to the victim using botnets or other amplification methods, exhausting the bandwidth between the target and larger network/internet. UDP protocol is commonly used to exploit any excessive increase in packet size. DNS amplification attacks perform service requests to change the source address field with the victim's address, causing response amplification by the servers and exhausting the victim bandwidth, as demonstrated in Figure 3 [37,40,41]. Similarly, ICMP floods send abnormal packets to target servers, making them inaccessible to legitimate requests [39–41].

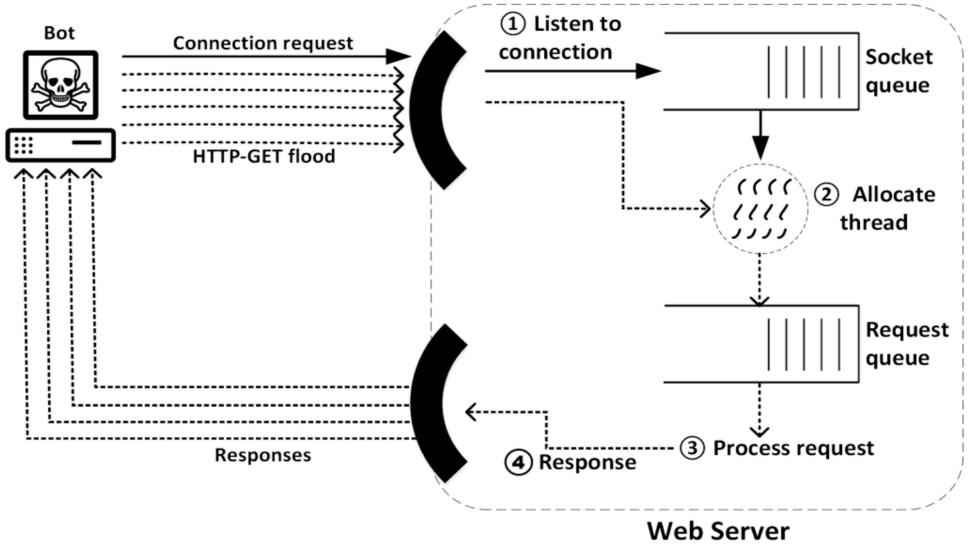

Figure 2. Application layer DDoS attack example [42].

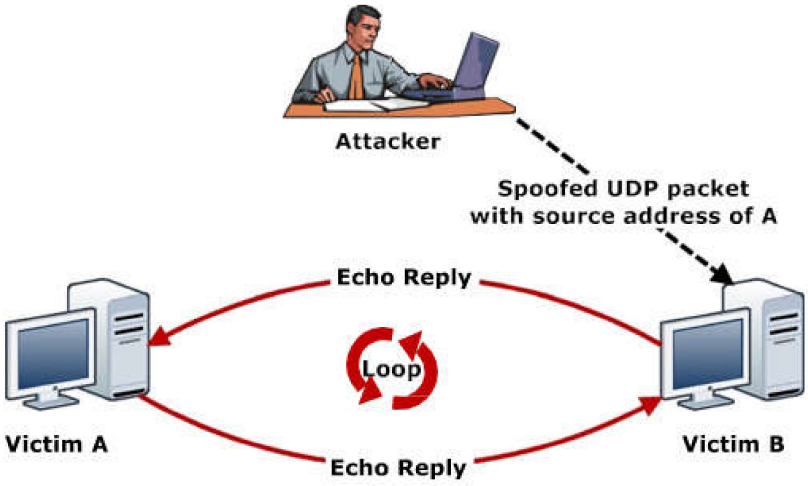

Figure 3. UDP Storm—volumetric attack example [43].

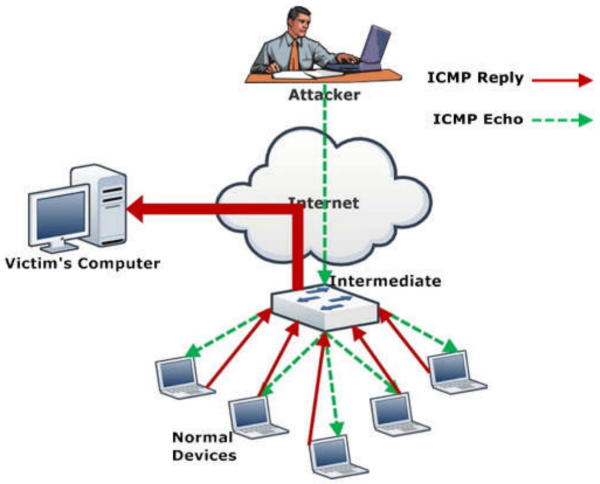

Figure 4. Smurf Attack—resource exhaustion attack example [43].

2.2. Blockchain

Blockchain aims at cryptographically secured list of records on globally available computing devices. These records are publicly certifiable, immutable and sequentially generated known as blocks. It is a distributed record keeping the ledger accessible to numerous nodes for record keeping. It is an interconnected chain of nodes starting with the genesis block with every next block, storing information about the previous node (see Figure 5). The nodes in this network possess the capability of accepting or rejecting data transactions by constantly observing the data blocks. Each record in these blocks is timestamped and added upon verification throughout the chain. Cryptographic hash functions map a random size input message to a fixed size output message given by $\{0,1\}^* - \{0,1\}^n$ [44]. While it might not replace the traditional information sharing mechanisms completely, it represents a new paradigm in secure verifiable and immutable information sharing.

The blockchain is based on the following significant building blocks: database, block, hash, miner, transaction and consensus mechanism [45].

1. Database: This aspect covers blockchains' fundamental capability or buildup of storing the information in a non-traditional method and structure (rows and columns). It stores all transaction records of the participating users with high throughput, no central control and immutable records, among others.
2. Blocks: Blocks store data associated with different transactions among the participating users. They are chained together storing hash values of previous blocks, forming a loop of tightly interconnected data. Typically divided into two, the header contains information about the block in the chain, while the latter part is associated with storing the actual transactional data [45,46].
3. Hash: These are complex mathematical problems responsible for identification and verification. Miners must solve these problems in order to trace a block, while the hash function for two messages cannot be the same, allowing verification. A hash table is maintained for efficient indexing while the next blocks store hashes of previous blocks in the chain [45,47,48].
4. Miner: A network node that solves a computational problem locating a new block is referred as a block miner. New transactions are broadcasted across the chain, and participants efforts are rewarded based on proof-of-work. The generated block is accepted into the chain when the miners start working on the next block, so that the previous hash is stored, ensuring continuity of the chain [45,47].
5. Transaction: This is the smallest amount of task information stored in a block once verified by majority participants in the chain. The records are accessible throughout while being immutable [45,48]. Figure 5 is a detailed infographic about transaction execution flow inside a blockchain.
6. Consensus: Consensus over records is a key characteristic in blockchain achieved via various consensus mechanism. The famous ones are Proof of Work (PoW) and Proof of Stake (PoS); the former ones reward based on proof of the work for block generation while the latter distributes work based on a participant's virtual currency tokens [45,46].

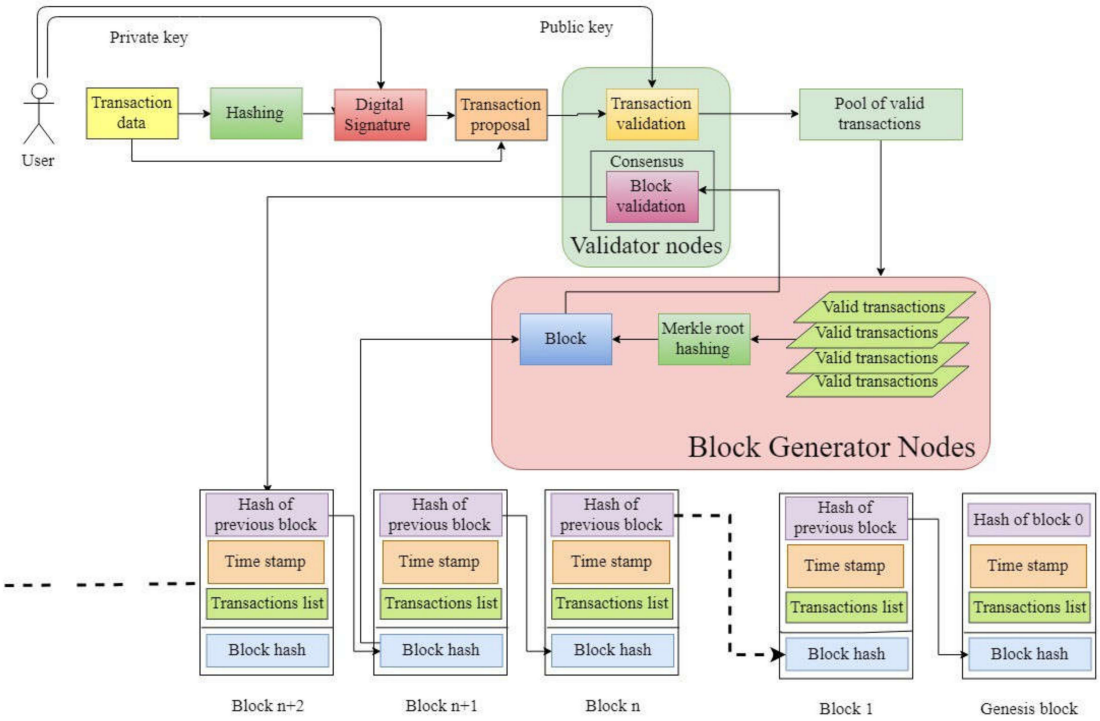

Figure 5. Transaction execution flow in a blockchain [49].

3. Review Methodology

The step-wise review methodology employed for this study is as follows:

1. Selection of relevant and appropriate digital libraries for search of relevant literature.
2. Design and refinement of search terms based on essential keywords concerning the subject of the study.
3. Refinement of retrieved results based on relevant search filters to studies associated with the domain.
4. Selection of studies defining inclusion and exclusion criteria based on title, abstract, keywords and content.

3.1. Sources

Scopus (https://www.scopus.com) indexes all major relevant digital libraries and journals in computer science and engineering. It also has a user-friendly and comprehensive search design. Therefore, it was used as the primary search engine for this review.

3.2. Search Methodology:

The search for relevant literature can be summed up in the following steps:

1. The search term was based on the keywords that directly relate to the topic under discussion. The search term used in this review was "DDoS" AND "Mitigation" AND "Using" AND "Blockchain" IN "All Fields", to include all possible studies relating to the keyword domains. The search retrieved a total of 368 research articles.
2. The following filters were applied to the retrieved results
    a. Limit by Subject Area—Results were filtered by *Computer Science* AND *Engineering* AND *Mathematics* AND *Decision Sciences* AND *Multidisciplinary*. A total of 359 documents were displayed. However, this study wanted to verify that the unrelated subject areas do not contain any related researches. Multiple related documents were found categorized in unrelated domains. Hence, the filter was removed, setting the number of primary documents back to 368.

b. Exclude by Document Type—Results were filtered by *Review* and *Conference Review*. However, in a separate search, these documents were checked to verify any reviews written in this domain. Exclusion yielded 317 documents.
c. Limit by Language—Filter results by *English*. Six items were dropped, leaving the number of items to 313 documents.

3.3. Inclusion and Exclusion Criteria

This review primarily selected documents based on titles and abstracts of the retrieved researches. However, no study was excluded only on the basis of title and abstract, unless a full text analysis deemed it irrelevant to the current review. The criteria are as follows:

1. Inclusion Criteria
    a. Studies reporting usage of blockchain for DDoS mitigation
    b. All studies in this domain to date were included (2015–2021)
2. Exclusion Criteria
    a. Studies reporting only DDoS or DDoS mitigation or blockchain
    b. Other surveys about DDoS mitigation
    c. Studies dealing with protection of blockchain or its applications
    d. Unavailable full prints such as Symposiums and Workshops
    e. Surveys were filtered during the search

Out of the 313 documents, 36 studies were chosen based on the aforementioned criterion. These 36 studies were analyzed, and a comprehensive review was presented in the proceeding section. They were further tabulated for ease of use highlighting essential points for almost all of them.

4. Comprehensive Review

The design of mitigation schemes usually involves multi-faceted architecture in an attempt to increase the effectiveness. Other methods/technologies have been used in association with blockchain. As such, the subsequent sections analyze the solutions reviewed by this study, categorized based on the dominant method/technology. The classification does not undermine the role of blockchain for DDoS mitigation in all the discussed approaches. A taxonomical flowchart was also proposed, as seen in Figure 6, for an intuitive understanding of the domain under discussion. The review is divided into six sub-sections as follows:

4.1. Software-Defined Networking (SDN)

Cochain-SC proposes network schemes governed by blockchain using SDN and smart contracts for DDoS mitigation at an inter and intra domain level. The Ethereum smart contract-based scheme helps multiple SDN-based domains to mitigate DDoS by sharing attack information. Intra domain DDoS attack detection is performed by an Intra Entropy-based scheme and Intra Bayes-based scheme by measuring the randomness and anomalies in the network traffic. The randomness is measured using sFlow, whereby it performs flow aggregation during the DDoS attack. The entropy calculation using Shannon's information theory measures the randomness of data based on the principle that the flow of traffic towards the victim's IP address increases substantially and is concentrated towards the victim, leading to an increase in the entropy. A binary machine learning classifier determines the change as legitimate or illegitimate. Suspected packets are dropped based on defined network rules for mitigation. The victim domain shares the information over the SDN-connected nodes where each SDN controller retrieves the list of illegitimate IPs for attack detection and mitigation. Experimental results indicated that the proposed setup is efficient and cost effective. The implementation is simulated using mininet, Scapy's Python library and Hping3 while keeping the attack rate between 100 to 500 Mbps [50].

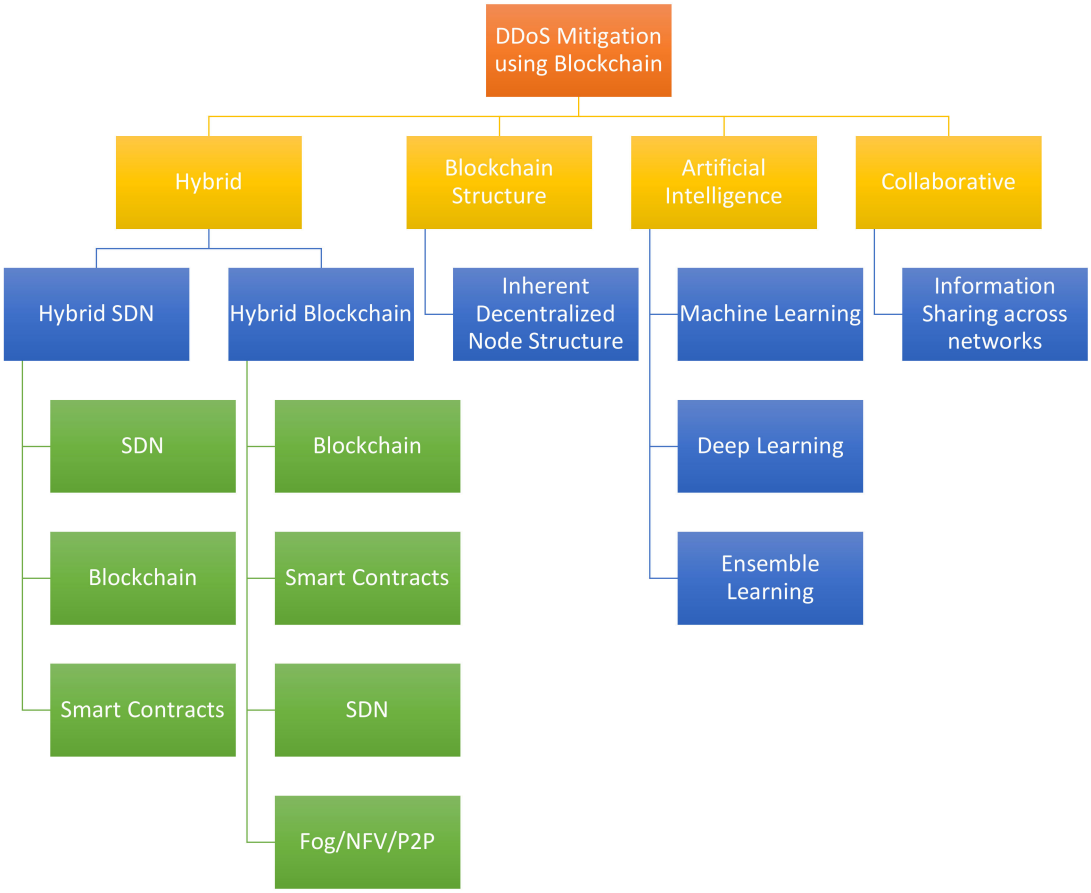

Figure 6. Proposed taxonomy.

Co-IoT leverages the SDN controller of the victim's network to detect and mitigate a DDoS attack in IoT devices. At the same time a domain-wide notification of the attacker is shared via an Ethereum smart contract. The remaining SDN nodes are thus ready to block any incoming traffic from the attack domain. The basic detection and mitigation schemes completely rely on efficiency of SDN controllers [51]. Similar work has been reported by [52]. A similar setup specifically for Mirai botnet is presented in [53], reporting a true detection rate of 95%. Simulations were conducted in a custom developed simulator in Java.

In [54], researchers presented a collaborative generic hardware and defense capability shared DDoS mitigation scheme. The framework includes software-defined networks for customized security policies in a software style for managing applications (Ryu-open source) and network function virtualization (sFlow or NetFlow) for enforcing the security policies using generic hardware, Ethereum-based blockchain for advertising and sharing near real time threat information (14 s, time to mine a block) and smart contracts dedicated to define the rules of collaboration and information sharing. The framework's major strength seems to be the usage of generic hardware through network function virtualization.

4.2. Blockchain and Smart Contracts

The centralized controller mechanism in resource-constrained SDNs make them prone to network attacks, including DDoS. A decentralized private blockchain can be used for setting flow rules for fog nodes acting as SDN controllers and other devices in the network. Private blockchain enables miners to revert to previous flow rules or blocks as soon as the miners detect faulty flow rules in the network. The data immutability of private blockchain does not guarantee its security from devices using the same hash key and genesis file. Enhanced encryption of the flow rules before block insertion is thus

required. The performance of such a setup was measured on a Raspberry Pi device as SDN controllers, machines with i5 processors as miners and the go-Ethereum-based private blockchain. Since the SDN control mechanism is decentralized, results demonstrate that other fog nodes are able to retract back to the previous flow as soon as one of the nodes is under attack. The deployment architecture in the fog layer helps to reduce the latency and energy consumption [55]. A distributed peer to peer network using blockchain to protect data integrity and confidentiality in enterprise networks was implemented in [56]. The hybrid architecture involves deployment of a smart contract using blockchain. Blockchain enables shared protection while smart contract distributes the rules among the host nodes in the network. It measures received response amount verses the predefined maximum response count. Any abnormalities are further inspected and the attacker IP address is blacklisted. Once the DDoS packet flooding is detected, mitigation script is activated leading to drop of packets to zero by blocking the blacklisted IP, indicating the success of the mitigation framework. Opendaylight and mininet are used for network setup, python for smart contracts while no information has been provided about blockchain except that it is private. A major limitation in this approach is the predefined packet response rate. Any packet transmission above the predefined rules, even legitimate, is likely to get blocked due to the nature of implementation. Reference [57] focuses on blockchain expansion inside an IoT network to securely store assets-configuration files from SDN or NFV. The problem domain is specifically expanding the blockchain in fog to avoid 51% attack so that the IoT network can be protected reliably using the blockchain. Blockchain is essentially used as a ledger in their network setup for user authentication as a protection against DDoS attacks. A similar conceptual framework was reported by [58] using SDN controllers imbedded in the smart contract for detection and mitigation. The information sharing is proposed at a global or intra level, similar to [50].

A public permissioned blockchain tries to fill in the gaps between public permissionless and private consortium networks in order to achieve the best of both models. A cyber threat intelligence platform using open-source permissioned blockchain is discussed in [59]. The blockchain is essentially used for record-keeping, and smart contracts are used to guarantee immutable logic. With software defined networking to enhance the mitigation, this serves as a collaborative platform for DDoS mitigation. The collaborative platform leverages blockchain capabilities of tamper proof data and secure information sharing between the network participants for the mitigation process. This has been implemented on a HLF blockchain to evaluate the performance in a multi domain SDN setup. The SDN setup is simulated using Kathara, Ryu and OpenVSSwitch on Ubuntu 16.04. The traffic is constantly monitored against a blacklist host log in HLF, which is continuously updated and shared among the network. On detection, the blacklisted IP is blocked instantaneously based on logical rules set up in the smart contract. Secure information sharing among collaborators is the essential mitigation mechanism. However, the results indicate decreased latency and transaction throughput, highlighting the need for high-power computing.

BlockSDSec uses blockchain as a service for DDoS mitigation in SDNs. The SDN framework uses OpenFlow (OF) protocol to establish communication between the controller and switches. The main idea is to use blockchain upon the OF switches to maintain data integrity from any form of tampering due to a DDoS attack while contacting the controller. Moreover, data from each layer for the SDN is also added to the block, ensuring integrity and validation. The entire experiment focuses on the deployment with no details of the testing scenario. Particularly, the setup has not been tested for DDoS resilience [60]. Similar data transfer at the OF level was reported in [61]. Blockchain networks at application level and device level were added in [62]. Each node is seemingly a part of the blockchain network possessing a unique hash and relative hashes. This helps the devices to recover from any falsified data without the controller's immediate attention. Implementation details are scarce and it most likely seems like a conceptual framework. A blockchain-based middle layer between infrastructure and control layers in UAV stores communication and

controller information, acting as a secure immutable and transparent middleman. Each communication is stored as a transaction on the nodes keeping track of any malicious UAV transmissions and avoiding single point failure [63].

Smart meters provide real time pricing, energy consumption, automate diagnostics, billing, monitoring, etc. These smart meters have been flooded with DDoS attacks making them new vectors for cyber-attacks. The centralized access control mechanism is at the core of these attacks. The paper presents a decentralized access control architecture using smart contracts on Ethereum. Blockchain-based access control is efficient and immutable. The decentralized architecture is implemented using Ropsten, Ethereum's official test net. All the smart devices are connected through a peer to peer network, while an access control contract is designed based on blockchain smart contract. This contract manages subject–object pairing through the defined rules. Any interaction/action between the subject and object is governed by the rules in the contract. The architecture was implemented and tested using the Ganache simulator and Ropsten, while the smart contract deployment used the truffle framework. The authors concluded that the decentralized access mechanism achieves higher security and efficiency in maintaining the network [64].

4.3. Blockchain Structure

A decentralized CDN mitigation scheme using private blockchain was discussed in [65]. The configuration consists of permission nodes acting as block generators using the Byzantine Fault Tolerance family algorithm. The bandwidth for node creation is provided by a separate set of nodes referred to as bandwidth nodes. It is important to distinguish between the two entities because it minimizes the possibilities of block modification while using bandwidth, ensuring the safety of the contract record and creation of reliable nodes. The structure is deemed robust as the integrity is tightly controlled by hub nodes in the decentralized structure. A major limitation of IoT networks is a centralized point of control which can be overcome using blockchain's decentralized properties. Each device is associated with a node in the blockchain containing hash and timestamp. All the information generated by the devices is associated with the respective block. Any information tampering following a network intrusion is detected by matching device data with the node data. Since the data on the node cannot be tampered, the IoT device and communication is reverted to the previous state, thereby protecting the data generated by IoT devices [66].

Reference [67] proposes a biologically inspired collaborative DDoS detection framework using blockchain, smart contract and fuzzy neural networks. Each collaborator is hosted on a private blockchain protecting their privacy and not sharing their data with other collaborators. Fuzzy neural networks are used in the smart contract to detect and filter the experimental results. Upon detection of abnormal data, the results are uploaded into a public blockchain accessible to all collaborators of the system. The users can download these results onto their private blocks requiring no direct communication between the participants. This experiment was conducted using the Hyperledger-fabric. Experimental results conclude that the system required an average of 1.66 ms to store each piece of information with detection accuracy of 0.89 and a recall of 0.87.

4.4. Artificial Intelligence

Machine learning techniques such as KNN, decision trees and random forest have proven capable of DDoS detection. Blockchain can be used to securely store the blacklisted IP addresses. An Ethereum-based blockchain running a smart contract storing the malicious IPs along with their timestamp is reported in [68]. The server is informed to block the associated traffic. The IP is unblocked automatically after a set threshold time by fetching the blocked IP from the blockchain ledger. The authors argue that the blockchain-based enhancement provides additional security to existing DDoS mitigation models. LSTM is used for DDoS detection utilizing blockchain for permission to edge devices to perform actions [69]. IoT devices are relatively unsecure compared to traditional network nodes.

The proposed model analyzes the network traffic on edge devices connected via blockchain. The analysis process yields abnormal behavioral patterns and implements the attack defense mechanism through smart contracts deployed over the nodes. Attacks are detected using the LSTM-based model. The system architecture leverages blockchain's resource owner control release in the first block and passes on based on request. The request is granted based on the access control policy stored inside the blockchain, granting automatic permissions to edge devices for actions over the blockchain network. A similar conceptual model is presented in [20] using SDN, RNN-LSTM and smart contracts.

Traditionally, software-defined industrial networks rely on a centralized controller, leading to an inevitable single point of failure due to a service denial attack. A deep learning-based blockchain framework, whereby switch authenticity is controlled by the blockchain and anomaly detection is done by a deep Boltzmann machine, is presented in [61]. Each switch is registered on the blockchain using the zero-knowledge proof concept and verified using consensus mechanisms. Deep learning-based models are deployed to identify characteristics of DDoS attacks over the network. The framework was tested using a mininet emulator—two servers for traffic flow generation and virtual PX as the DBM flow analyzer. The deep learning model was trained using the KDD dataset for anomaly detection in network systems. A 5–10% increase in detection efficiency was reported from the experiment, while the computational costs were comparatively higher than previous models.

A virtual parallel blockchain with heterogenous ensemble learning protects the actual blockchain-based network from direct DDoS attacks. The mechanism is based on creating an artificial blockchain based on virtual reality parallel tactics and connected to the original blockchain. DDoS detection and mitigation is guided by ensemble learning distributed over the virtual blockchain nodes. Since these blockchains are mirror copies of each other, the artificial blockchain effectively guides the detection and defense of DDoS attacks in actual blockchain. Learning transfer based on computation, experimentation and evaluation constantly optimizes the original blockchain for attack management. AdaBoost and random forest are used as ensemble learning strategies by integrating lightweight classifiers such as CART and ID3. The detection and mitigation strategy in artificial blockchain demonstrates good performance and optimizes and guides the original blockchain against the DDoS attacks effectively. The experimental results were demonstrated in the artificial blockchain, while the learning and optimization process of the original blockchain has not been verified experimentally [70].

4.5. Collaborative Platforms

BloSS is a cooperative and collaborative prototype for threat information sharing based on an incentive model using blockchain, smart contracts and software-defined networking. Collaborators post information about new threats on the blockchain whereby data is first stored in IPFS and the associated hash is stored in a block on Ethereum. Sensitive information is encrypted over the blockchain-based network as confidentiality and integrity are essential in any cooperative model. An experimental evaluation to determine cost–benefit analysis using Truffle and Ganache was conducted in [71]. A global simulation across geographical nodes was also conducted using AWS. This modeling has been proven successful on both local and global networks. [71,72]. A similar signaling mechanism, SC-FLARE, was separately presented by the authors in [73]. Participants usually lack motivation in cooperative defense systems. An incentive-based reputation mechanism for BloSS has been demonstrated in [74]. In a real-world setting, the final burden of rejecting traffic is on a cyber security analyst. Reference [75] proposes a visualization dashboard for BloSS. Distributed ledger technologies can be very useful for signaling, coordination and orchestration using blockchain-based smart contracts. SOChain's detection mechanism is based on constantly observing abnormal behavior in data by the host machines and determining the latest attack address. The study argues that unfair exchange of threat data is an impediment between security operation centers. SOChain is a decentralized

incentive-based data exchange platform where information sharing is rewarded using DDoS coin tokens. The blockchain-based platform helps to overcome trust and fairness issues. Partners can use bloom filters to search the threat data/IP addresses corresponding to irregularities or threats in their networks. A dual level bloom filter is also used to protect the privacy of the uploaded and purchased data between entities. Confidentiality is taken care of using Diffie–Hellman key-exchange and symmetric encryption, while integrity is assured using a signature method. The paper detailed the implementation of each filter and exchange level [76]. The authors in [77] employed a ranking mechanism focused on network providers sharing information in a trust federation. Once the DDoS attack is detected by an external agent, information sharing takes place over the blockchain network, assigning reputation scores based on historical information. Reputation scores determine the allocation of resources for attack defense, and the mitigation is assigned to express the data path framework. Blockchain is essentially used to store and share information for collaborative scoring before any mitigation process is deployed. DefenseChain is another consortium for threat intelligent sharing and works on an incentive basis between organizations for effective impact on the mitigation process. The platform comparatively requires fewer resources and shorter duration for deployment. The setup is based on Dolus defense by pretense implementation. The implementation involves the NSF cloud whereby information is shared and incentivized after threat detection by Ferntic using Python. DefenseChain involves multiple stage detection and mitigation in terms of policy update, attack traffic redirection and spoofing, which makes it slower compared to similar models. Despite the detection mitigation time factor, the re-occurrence rate is quite lower [78]. A collaborative system employing encrypted IP lists using an AES algorithm into a swarm and a distributed file storage system embedded in Ethereum is reported in [79]. The blockchain hashing function guarantees tamper proof lists. Compared to other similar systems, researchers propose to store only hash values in the smart contract, which is transparent in nature. Instead they store the encrypted IPs in the swarm and provide URLs for participants to check the IP list. The smart contract is used to determine potential DDoS sources by comparing the information provided by different collaborators. Once similar IPs are detected from multiple sources, these are flagged as potential threats. While the smart contract comparison is similar to a consensus protocol, attack botnets emerge from scrambled and different IPs in different attacks. This becomes a major limitation of the proposed approach. An agent is allocated at each node consisting of multiple IoT devices and shares outbound traffic information with others to identify possible DDoS attacks. This information exchange uses a smart contract to ensure integrity of the cooperation and information in IoT networks [80]

Insider threats are one of the major issues in IoT sensor-based networks. Researchers investigate the effect of environment tampering on the perception layer and propose an Ethereum-based framework deploying smart contracts and edge computing, which validates the incoming data. This helps in preserving the data integrity for accurate analytics and processing. Ethereum is deployed on each edge node by selecting only one candidate for proof of work while distributing the processing results to all the nodes in the chain. A smart contract is written to validate the data integrity of the incoming sensor data, and faulty values are corrected using standard environmental conditions. Any insider tampering is corrected and registered with details, such as timestamp, for analysis. The experiment was conducted on a low computation power machine and Marvin, which signifies its scalability. Testing concluded change of faulty data to standard operating values before forwarding them for analytical processes [81]; this study did not specifically deal with DDoS mitigation. However, similar strategies have been used by other researchers for DDoS detection in an IoT-based network.

Table 1 presents an overview, highlights major findings and comments on crucial issues surrounding the studies included in this review, to pave the way for future research in this domain.

Table 1. Review overview.

Contributor	Purpose of Study	Method/s	Findings	Comments
[50]	Low cost and flexible DDoS mitigation scheme	Entropy, machine learning, blockchain and smart contracts	The scheme is successful in mitigating intra DDoS attacks using entropy changes and machine learning while inter domain attacks are catered by information sharing through smart contracts	A distributed DDoS attack within the same domain will affect the entropy measurement while a coordinated inter DDoS attack renders the smart contract layer less effective. The solution is scalable when the attack is specified to a specific entity within a particular SDN
[51,52]	Low cost, efficient and flexible collaborative DDoS mitigation platforms	SDNs and smart contract	The collaboration using smart contract is efficient and cost effective over all	The efficiency of mitigation is primarily dependent on SDN controllers. Blockchain is only used for attacker information sharing
[53]	Mitigation against Mirai botnet attack			
[54]	Collaborative multi-domain DDoS mitigation	SDN, NFV, blockchain and smart contracts	The framework provides a multi domain collaborative structure to reduce the DDoS mitigation burden by using SDN, NFV and blockchain	No experimental proof to indicate the performance of the proposed framework The detection model is still based on traditional traffic comparison
[55]	Decentralizing a single point of failure in resource constrained SDNs	Blockchain decentralization	Successfully revert back to previous flow/block on detection	Detection is based on a set rule flow comparison
[56]	Protection of enterprise networks against DDoS	Hybrid method in SDNs using blockchain	Illegitimate packet drop upon DDoS detection	No information about the private blockchain type No details about the blockchain application or smart contract Legitimate packet with higher transmission rate than predefined rule is most likely to get blocked
[57]	Blockchain expansion for securing configuration files against DDoS attacks	Blockchain and smart contract	Blockchain effectively secures the transaction details in fog networks. Any attempt to change transactional data is thwarted using blockchain-based network setup	Blockchain is only used as a record keeper
[58]			A hybrid of [50,57]	
[59]	Design a collaborative DDoS mitigation platform using blockchain, smart contract and SDNs	Hybrid approach	Instant DDoS mitigation by threat tracing	The threat host log must already contain information to detect a DDoS attack The simulated setup is not scalable for real world environment Blockchain is only used for storing and sharing threat data–blacklisted IPs

Table 1. *Cont.*

Contributor	Purpose of Study	Method/s	Findings	Comments
[60]	Overcoming single point of failure in SDNs	Blockchain	Blockchain can ensure integrity and validity of data travelling between layers	No experimental proof for DDoS mitigation The implementation focuses only on the setup Experimental setup and results are not clearly presented
[62]	Overcoming a single point of failure in SDNs	Blockchain	Each node is embedded in a blockchain network securing the data from tampering	Implementation details are scarce and therefore the validity cannot be determined Additional time cost in the network due to implementation of blockchain at each node
[63]	Blockchain enabled secure middle layer to avoid single point failure	Communication layer based on blockchain	The blockchain middle layer protects data and helps to avoid single point failure	Theoretical framework with no implementation. As such, no results are included
[64]	Prevention of cyber-attacks on smart meters	Decentralized access control policy using Ethereum smart contracts	Higher security, flexibility and efficiency	There seems to be no experimental results to indicate higher security
[65]	Vulnerability of DDoS mitigation schemes due to centralization	Private blockchain and scale free networks	Higher reliability and permissibility of nodes as the integrity is tightly controlled by hub nodes in the decentralized structure.	Theoretical referring to graph theory with no implementation or experimental results.
[66]	Securing data generated by IoT devices	IoT device data validation with associated blockchain nodes	Data tampering is detected instantly in IoT devices and healed using stored information across various blockchain nodes	The focus is on the security of data generated by IoT devices rather than DDoS or threat mitigation
[67]	Collaborative detection system using public and private blockchain	Private entity data and public threat data over blockchain	Fuzzy neural networks over smart contracts are used for threat detection which is shared over the public blockchain for collaborators to download to their private blocks	Non-real-time threat information sharing might paralyze the architecture in case of a coordinated attack on multiple private chains
[68]	Enhanced DDoS mitigation model	Secure and accessible information sharing over smart contract	Malicious node information being available to all nodes enhances current DDoS mitigation models	Largely dependent on the machine learning detection to categorize traffic No details about the threshold time for blacklisted IP releaseBlacklisted IP release may also indicate extra burden on the network as paper does not provide any key information about the underlying rules
[69]	DDoS defense method for IoT devices	Hybrid method using LSTM and smart contracts	Conceptual mitigation model	No experimental proof

Table 1. *Cont.*

Contributor	Purpose of Study	Method/s	Findings	Comments
[20]	DDoS mitigation	SDN, RNN-LSTM and smart contracts		Purely conceptual Usage of outdated DDoS datasets for deep learning detection model Finite or infinite duration for smart contracts implies constant involvement of fixed parties A decentralized model replacement for smart contracts is more viable to avoid fixed participation and avoid financial implications
[61]	Avoid single point of failure in software-defined industrial networks	Deep learning and blockchain-based DDoS defense	Switch registration and verification is secured over the blockchain and deep Boltzmann machine helps in anomaly detection. There is a significant increase in detection efficiency	Computation and communication cost are higher Simulation-based environment, yet to scale to a real-world industrial network to test the detection efficiency
[70]	DDoS defense in blockchain	Virtual artificial blockchain	Using ensemble strategy in artificial blockchain, the defense mechanism performs very well	No learning and optimization from virtual blockchain to original blockchain has been demonstrated experimentally
[71–73]	Collaborative threat information sharing	Incentivized information sharing	Incentivized cooperative model based on blockchain is economically and geographically beneficial as a threat signaling system	Improvements to threat information storage and incentive model can be made further Blockchain is essentially used for information sharing
[74]	Enhancement: Incentive Scheme for [71]. Applicable to [72,73].			
[75]	Enhancement: Visualization scheme for [71]. Applicable to [72,73].			
[76]	Incentivized DDoS threat information sharing exchange service	Blockchain-based information sharing and coin-based incentives	Threat information sharing is rewarded using coins and reputation while a novel double bloom filter protects buyer and seller privacy	Upload computational cost is slightly higher than TRAD The computational costs were calculated using server-based setup. Computation power still largely impacts performance rate in blockchains
[77]	Handling DDoS mitigation for network service providers	eXpress Data Path framework, blockchain is being used for data storage and sharing	Due to the nature of data, mitigation is almost 100%	The mitigation filters are already classified in the dataset detecting all malicious trafficA real-world test has not been demonstrated Does not focus on detection Blockchain is not used for mitigation
[78]	Threat Intelligence Sharing Consortium	Information about malicious blacklisted hosts securely through blockchain	Blockchain stores and shares the information securely, helping to create an intelligent incentivized model reducing the impact of cyber-attacks and the reoccurrence rate	Time consuming detection and mitigation Blockchain is only used for information sharing

Table 1. *Cont.*

Contributor	Purpose of Study	Method/s	Findings	Comments
[79]	Information sharing between SOCs based on CIA triad and traceability	Blockchain, smart contract, elliptic curve Diffie–Hellman (ECDH) and elliptic curve Elgamal	A different storage model on the swarm with hashes in the smart contract is a securer way to store suspected IPs	Attack botnets emerge from scrambled and different IPs in different attacks There is no trust management between the collaborating entities as proposed in similar systems
[80]	Protect low power IoT devices against DDoS attacks	Multi-agent systems, consensus and smart contract	Agent collaboration is able to detect DDoS attack using consensus mechanism	Blockchain is only used to maintain the information integrity and govern the exchange Consensus mechanism needs to be tested on limited resource hardware The proposed framework has not been implemented on a blockchain network to prove its validity The research is focused mainly on the consensus mechanism
[81]	Protect integrity of sensor data in IoT perception layer based on insider threats	Smart contracts for data correction	Blockchain-based smart contracts were able to correct faulty data before passing it to the next layer Framework has a minimum execution cost as proof of work is restricted to one node at a time	Standard definitions inside the smart contract will correct values outside the range even if the sensor data is an accurate outlier

5. Discussion—Open Challenges and Opportunities

The study revealed that the contemporary mitigation solutions are mostly applicable to specific scenarios or architectures. Some of the ideas are promising yet conceptual in nature without any experimental proofs and require further research to prove their validity and effectiveness for DDoS mitigation. Another open challenge is scalability of these solutions to real world settings, which still remains to be studied. At the same time, the data used in some of the learning approaches is outdated, which complicates the effectiveness of such solutions. As the complexity and volume of DDoS attacks has increased over the years, the current solutions or any future work need to be evaluated based on realistic scenarios. Simulation environments must be able to mimic real world or near real world conditions both in terms of traffic and infrastructure. Predefined rules will cater only to already reported attacks while leaving the networks still vulnerable to new attacks. Dynamic learning approaches updated at short regular intervals must be studied. The mitigation architectures need to be implemented at a protocol level so that they are inherent into the network architecture providing them greater inbuilt control over the traffic flow rather than being bystanders waiting for protocol execution before taking necessary measures for mitigation. The implementation at the protocol level will likely generalize the implementation of such solutions across various network domains and architectures. The inherent architecture of blockchain must also be studied and leveraged for effective mitigation solutions. Other emerging technologies such as network function virtualization, fog computing, edge computing, etc. must be included in the hybrid architecture of blockchain-based mitigation solutions.

6. Conclusions

The complexity of DDoS attacks has led to a considerable amount of losses, financially and computationally, and especially service denial. The projected numbers indicate a manifold increase in the next few years. The ever-increasing reliance on cyber physical

systems and constant evolution of DDoS attacks demand innovative and more efficient solutions for DDoS detection and mitigation. Blockchains' inherent characteristics have proven to be a major leap in this domain. However, appropriate attention has not been given towards blockchain technology for cybersecurity, especially DDoS mitigation. As such, there is an immediate need to discuss the advancements in this area so that more focused research is directed to solve the critical issues at hand. This study provided a comprehensive review of all related works to DDoS mitigation strategies using blockchain. The discussion provided all relevant details of these approaches at one place and provided an overview of related methods and techniques in light of each other. A review overview was tabulated, highlighting the major findings and commenting on crucial issues surrounding these studies to pave the way for future research in this domain. A brief taxonomical approach was illustrated to provide an overview of the structure of mitigation solutions under review. Finally, limitations and opportunities were discussed in the preceding section. The discussion clearly indicates that this domain of research is still in its infancy, and blockchain has not been leveraged to its best potential to solve issues pertinent to DDoS mitigation.

Author Contributions: Conceptualization, S.W.; methodology, S.W. and S.A.; validation, K.M.A., S.A. and Y.G.; formal analysis, S.W. and S.A.; investigation, S.W.; resources, S.W., M.I., and H.A.; data curation, S.W. and K.M.A.; writing—original draft preparation, S.W. and M.I.; writing—review and editing, S.W., H.A. and Y.G.; visualization, S.W.; funding acquisition, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been funded by Deanship of Scientific Research at Majmaah University under project number NO (R-2021-7). The authors extend their special appreciation to the Deanship for their support to publish this work.

Acknowledgments: The authors would like to thank the reviewers for their valuable feedback. We would also like to thank International Islamic University Malaysia and the Deanship of Scientific Research at Majmaah University for their support towards the completion of this work.

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

References

1. Agrawal, N.; Tapaswi, S. Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 3769–3795. [CrossRef]
2. Banitalebi Dehkordi, A.; Soltanaghaei, M.R.; Boroujeni, F.Z. The DDoS attacks detection through machine learning and statistical methods in SDN. *J. Supercomput.* **2020**, 1–33. [CrossRef]
3. Fazeldehkordi, E.; Owe, O.; Ramezanifarkhani, T. A Language-Based Approach to Prevent DDoS Attacks in Distributed Financial Agent Systems. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 11981, pp. 258–277. [CrossRef]
4. Singh, K.; Dhindsa, K.S.; Nehra, D. T-CAD: A threshold based collaborative DDoS attack detection in multiple autonomous systems. *J. Inf. Secur. Appl.* **2020**, *51*, 102457. [CrossRef]
5. Cheng, J.; Li, J.; Tang, X.; Sheng, V.S.; Zhang, C.; Li, M. A novel DDoS attack detection method using optimized generalized multiple kernel learning. *Comput. Mater. Contin.* **2020**, *62*, 1423–1443. [CrossRef]
6. Mirchev, M.J.; Mirtchev, S.T. System for DDoS attack mitigation by discovering the attack vectors through statistical traffic analysis. *Int. J. Inf. Comput. Secur.* **2020**, *13*, 309–321. [CrossRef]
7. Lotfalizadeh, H.; Kim, D.S. Investigating Real-Time Entropy Features of DDoS Attack Based on Categorized Partial-Flows. In Proceedings of the 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM), Taichung, Taiwan, 3–5 January 2020. [CrossRef]
8. Abubakar, R.; Aldegheishem, A.; Faran Majeed, M.; Mehmood, A.; Maryam, H.; Ali Alrajeh, N.; Maple, C.; Jawad, M. An Effective Mechanism to Mitigate Real-Time DDoS Attack. *IEEE Access* **2020**, *8*, 126215–126227. [CrossRef]
9. Yuan, B.; Zhao, H.; Lin, C.; Zou, D.; Yang, L.T.; Jin, H.; He, L.; Yu, S. Minimizing Financial Cost of DDoS Attack Defense in Clouds with Fine-Grained Resource Management. *IEEE Trans. Netw. Sci. Eng.* **2020**. [CrossRef]
10. Khooi, X.Z.; Csikor, L.; Divakaran, D.M.; Kang, M.S. DIDA: Distributed in-Network Defense Architecture against Amplified Reflection DDoS Attacks. In Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridging the Gap Between AI and Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; pp. 277–281. [CrossRef]
11. Wang, A.; Chang, W.; Chen, S.; Mohaisen, A. A Data-Driven Study of DDoS Attacks and Their Dynamics. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 648–661. [CrossRef]

12. Saxena, U.; Sodhi, J.S.; Singh, Y. An Analysis of DDoS Attacks in a Smart Home Networks. In Proceedings of the Confluence 2020—10th International Conference on Cloud Computing, Data Science and Engineering, Noida, India, 29–31 January 2020; pp. 272–276. [CrossRef]
13. Kotey, S.; Tchao, E.; Gadze, J. On Distributed Denial of Service Current Defense Schemes. *Technologies* **2019**, *7*, 19. [CrossRef]
14. Choi, S.; An, Y.; Sasase, I. A Lightweight Detection Using Bloom Filter against Flooding DDoS Attack. *IEICE Trans. Inf. Syst.* **2020**, *103*, 2600–2610. [CrossRef]
15. NETSCOUT. High-Profile DDoS Extortion Attacks—September 2020. Available online: https://www.netscout.com/blog/asert/high-profile-ddos-extortion-attacks-september-2020 (accessed on 14 January 2021).
16. Cisco Annual Internet Report—Cisco Annual Internet Report (2018–2023) White Paper—Cisco. Available online: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed on 18 January 2021).
17. Ko, I.; Chambers, D.; Barrett, E. Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain. *ETRI J.* **2019**, *41*, 574–584. [CrossRef]
18. Mohammed, S.S.; Hussain, R.; Senko, O.; Bimaganbetov, B.; Lee, J.Y.; Hussain, F.; Kerrache, C.A.; Barka, E.; Alam Bhuiyan, M.Z. A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network. In Proceedings of the International Conference on Wireless and Mobile Computing, Networking and Communications, Limassol, Cyprus, 15–17 October 2018. [CrossRef]
19. Ko, I.; Chambers, D.; Barrett, E. Adaptable feature-selecting and threshold-moving complete autoencoder for DDoS flood attack mitigation. *J. Inf. Secur. Appl.* **2020**, *55*. [CrossRef]
20. Essaid, M.; Kim, D.Y.; Maeng, S.H.; Park, S.; Ju, H.T. A Collaborative DDoS Mitigation Solution Based on Ethereum Smart Contract and RNN-LSTM. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium: Management in a Cyber-Physical World (APNOMS 2019), Matsue, Japan, 18–20 September 2019. [CrossRef]
21. Ko, I.; Chambers, D.; Barrett, E. Feature Dynamic Deep Learning Approach for DDoS Mitigation within the ISP Domain. In Proceedings of the International Journal of Information Securitym; Springer: Berlin/Heidelberg, Germany, 2020; Volume 19, pp. 53–70. [CrossRef]
22. Simpson, K.A.; Rogers, S.; Pezaros, D.P. Per-Host DDoS Mitigation by Direct-Control Reinforcement Learning. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 103–117. [CrossRef]
23. Hugues-Salas, E.; Ntavou, F.; Ou, Y.; Kennard, J.E.; White, C.; Gkounis, D.; Nikolovgenis, K.; Kanellos, G.; Erven, C.; Lord, A.; et al. Experimental demonstration of DDoS mitigation over a Quantum key distribution (QKD) network using Software Defined Networking (SDN). In Proceedings of the 2018 Optical Fiber Communications Conference and Exposition (OFC), San Diego, CA, USA, 11–15 March 2018. Available online: https://ieeexplore.ieee.org/document/8385709 (accessed on 28 January 2021).
24. Harikrishna, P.; Amuthan, A. SDN-based DDoS Attack Mitigation Scheme using Convolution Recursively Enhanced Self Organizing Maps. *Sadhana Acad. Proc. Eng. Sci.* **2020**, *45*. [CrossRef]
25. Huong, T.T.; Thanh, N.H. Software defined networking-based One-packet DDoS mitigation architecture. In Proceedings of the 11th International Con-ference on Ubiquitous Information Management and Communication (IMCOM 2017), Beppu, Japan, 5–7 January 2017. Available online: https://dl.acm.org/doi/abs/10.1145/3022227.3022336 (accessed on 28 January 2021).
26. Hameed, S.; Khan, H.A. Leveraging SDN for Collaborative DDoS Mitigation. In Proceedings of the 2017 International Conference on Networked Systems (NetSys 2017), Gottingen, Germany, 13–16 March 2017. [CrossRef]
27. Hameed, S.; Khan, H.A. SDN based collaborative scheme for mitigation of DDoS attacks. *Futur. Internet* **2018**, *10*, 23. [CrossRef]
28. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Buyya, R. Service resizing for quick DDoS mitigation in cloud computing environment. *Ann. Telecommun. Telecommun.* **2017**, *72*, 237–252. [CrossRef]
29. Kuka, M.; Vojanec, K.; Kucera, J.; Benacek, P. Accelerated DDoS Attacks Mitigation Using Programmable Data Plane. In Proceedings of the 2019 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2019), Cambridge, UK, 24–25 September 2019. [CrossRef]
30. Ko, I.; Chambers, D.; Barrett, E. Self-supervised network traffic management for DDoS mitigation within the ISP domain. *Futur. Gener. Comput. Syst.* **2020**, *112*, 524–533. [CrossRef]
31. Ko, I.; Chambers, D.; Barrett, E. A Lightweight DDoS Attack Mitigation System within the ISP Domain Utilising Self-Organizing Map. In Proceedings of the Advances in Intelligent Systems and Computing; Springer: Berlin/Heidelberg, Germany, 2019; Volume 881, pp. 173–188. [CrossRef]
32. Bulbul, N.S.; Fischer, M. SDN/NFV-Based DDoS Mitigation via Pushback. In Proceedings of the IEEE International Conference on Communications, Dublin, Ireland, 7–11 June 2020. [CrossRef]
33. Beigi-Mohammadi, N.; Barna, C.; Shtern, M.; Khazaei, H.; Litoiu, M. CAAMP: Completely Automated DDoS Attack Mitigation Platform in Hybrid Clouds. In Proceedings of the 2016 12th International Conference on Network and Service Management (CNSM), Montreal, QC, Canada, 31 October–4 November 2016; pp. 136–143. [CrossRef]
34. Fulber Garcia, V.; De Freitas Gaiardo, G.; Da Cruz Marcuzzo, L.; Ceretta Nunes, R.; Paula Dos Santos, C.R. DeMONS: A DDoS Mitigation NFV Solution. In Proceedings of the Proceedings—International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 16–18 May 2018; pp. 769–776. [CrossRef]
35. Zhou, L.; Guo, H.; Deng, G. A fog computing based approach to DDoS mitigation in IIoT systems. *Comput. Secur.* **2019**, *85*, 51–62. [CrossRef]

36. Lohachab, A.; Karambir, B. Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks. *J. Commun. Inf. Netw.* **2018**, *3*, 57–78. [CrossRef]
37. Dantas Silva, F.S.; Silva, E.; Neto, E.P.; Lemos, M.; Venancio Neto, A.J.; Esposito, F. A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios. *Sensors* **2020**, *20*, 3078. [CrossRef]
38. Srinivasan, K.; Mubarakali, A.; Alqahtani, A.S.; Dinesh Kumar, A. A Survey on the Impact of DDoS Attacks in Cloud Computing: Prevention, Detection and Mitigation Techniques. In *Lecture Notes on Data Engineering and Communications Technologies*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 33, pp. 252–270.
39. Adhikary, K.; Bhushan, S.; Kumar, S.; Dutta, K. Hybrid Algorithm to Detect DDoS Attacks in VANETs. *Wirel. Pers. Commun.* **2020**, *114*, 3613–3634. [CrossRef]
40. Vishwakarma, R.; Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommun. Syst.* **2020**, *73*, 3–25. [CrossRef]
41. Azahari Mohd Yusof, M.; Hani Mohd Ali, F.; Yusof Darus, M. Detection and Defense Algorithms of Different Types of DDoS Attacks. *Int. J. Eng. Technol.* **2018**, *9*, 410–444. [CrossRef]
42. Singh, K.; Singh, P.; Kumar, K. Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. *Comput. Secur.* **2017**, *65*, 344–372. [CrossRef]
43. Gupta, B.B.; Badve, O.P. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment. *Neural Comput. Appl.* **2017**, *28*, 3655–3682. [CrossRef]
44. Alkadi, O.; Moustafa, N.; Turnbull, B. A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions. *IEEE Access* **2020**, *8*, 104893–104917. [CrossRef]
45. Atlam, H.F.; Wills, G.B. Technical aspects of blockchain and IoT. In *Advances in Computers*; Academic Press: Amsterdam, The Netherlands, 2019; Volume 115, pp. 1–39. ISBN 9780128171899. [CrossRef]
46. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Futur. Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
47. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction—Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder—Google Books. Available online: https://books.google.com.my/books?hl=en&lr=&id=LchFDAAAQBAJ&oi=fnd&pg=PP1&dq=Bitcoin+and+Cryptocurrency+Technologies&ots=AslEeY0InJ&sig=Rvnpl7K-O4XsMte7sftyGMYmbzU&redir_esc=y#v=onepage&q=BitcoinandCryptocurrencyTechnologies&f=false (accessed on 15 January 2021).
48. Peters, G.W.; Panayi, E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. *New Econ. Wind.* **2016**, 239–278. [CrossRef]
49. Ismail, L.; Materwala, H. A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry* **2019**, *11*, 1198. [CrossRef]
50. Abou El Houda, Z.; 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* **2019**, *7*, 98893–98907. [CrossRef]
51. El Houda, Z.A.; Hafid, A.; Khoukhi, L. Co-IoT: A Collaborative DDoS Mitigation Scheme in IoT Environment Based on Blockchain Using SDN. In Proceedings of the 2019 IEEE Global Communications Conference, GLOBECOM 2019—Proceedings, Waikoloa, HI, USA, 9–13 December 2019. [CrossRef]
52. Rodrigues, B.; Bocek, T.; Lareida, A.; Hausheer, D.; Rafati, S.; Stiller, B. A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10356, pp. 16–29. [CrossRef]
53. Ahmed, Z.; Danish, S.M.; Qureshi, H.K.; Lestas, M. Protecting IoTs from Mirai Botnet Attacks Using Blockchains. In Proceedings of the IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 11–13 September 2019.
54. Rodrigues, B.; Bocek, T.; Stiller, B. Multi-Domain DDoS Mitigation Based on Blockchains. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Limassol, Cyprus, 11–13 September 2019; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10356, pp. 185–190.
55. Misra, S.; Deb, P.K.; Pathak, N.; Mukherjee, A. Blockchain-Enabled SDN for Securing Fog-Based Resource-Constrained IoT. In Proceedings of the IEEE INFOCOM 2020–IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 490–495. [CrossRef]
56. Giri, N.; Jaisinghani, R.; Kriplani, R.; Ramrakhyani, T.; Bhatia, V. Distributed Denial of Service(DDoS) Mitigation in Software Defined Network using Blockchain. In Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud (I-SMAC), Palladam, India, 12–14 December 2019; pp. 673–678. [CrossRef]
57. Gul, M.J.; Rehman, A.; Paul, A.; Rho, S.; Riaz, R.; Kim, J. Blockchain Expansion to secure Assets with Fog Node on special Duty. *Soft Comput.* **2020**, *24*, 15209–15221. [CrossRef]
58. Al-Sakran, H.; Alharbi, Y.; Serguievskaia, I. Framework Architecture for Securing Iot Using Blockchain, Smart Contract and Software Defined Network Technologies. In Proceedings of the 2019 2nd International Conference on New Trends in Computing Sciences (ICTCS), Amman, Jordan, 9–11 October 2019. [CrossRef]
59. Hajizadeh, M.; Afraz, N.; Ruffini, M.; Bauschert, T. Collaborative Cyber Attack Defense in SDN Networks Using Blockchain Technology. In Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridging the Gap Between AI and Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; pp. 487–492. [CrossRef]

60. Bose, A.; Aujla, G.S.; Singh, M.; Kumar, N.; Cao, H. Blockchain as a Service for Software Defined Networks: A Denial of Service Attack Perspective. In Proceedings of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 5–8 August 2019; pp. 901–906.
61. Singh, M.; Aujla, G.S.; Singh, A.; Kumar, N.; Garg, S. Deep-Learning-Based Blockchain Framework for Secure Software-Defined Industrial Networks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 606–616. [CrossRef]
62. Lokesh, B.; Rajagopalan, N. A Blockchain-Based Security Model for SDNs. In Proceedings of the CONECCT 2020—6th IEEE International Conference on Electronics, Computing and Communication Technologies, Bangalore, India, 2–4 July 2020. [CrossRef]
63. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. A taxonomy of blockchain-enabled softwarization for secure UAV network. *Comput. Commun.* **2020**, *161*, 304–323. [CrossRef]
64. El Houda, Z.A.; Hafid, A.; Khoukhi, L. Blockchain Meets AMI: Towards Secure Advanced Metering Infrastructures. In Proceedings of the IEEE International Conference on Communications, Dublin, Ireland, 7–11 June 2020. [CrossRef]
65. Kim, K.; You, Y.; Park, M.; Lee, K. DDoS Mitigation: Decentralized CDN Using Private Blockchain. In Proceedings of the International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 3–6 July 2018; 2018; pp. 693–696. [CrossRef]
66. Sharma, R.K.; Pippal, R.S. Malicious Attack and Intrusion Prevention in IoT Network Using Blockchain Based Security Analysis. In Proceedings of the Proceedings—2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 25–26 September 2020; pp. 380–385. [CrossRef]
67. Han, X.; Zhang, R.; Liu, X.; Jiang, F. Biologically Inspired Smart Contract: A Blockchain-Based DDoS Detection System. In Proceedings of the 2020 IEEE International Conference on Networking, Sensing and Control (ICNSC), Nanjing, China, 30 October–2 November 2020. [CrossRef]
68. Manikumar, D.V.V.S.; Maheswari, B.U. Blockchain Based DDoS Mitigation Using Machine Learning Techniques. In Proceedings of the 2nd International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 15–17 July 2020; pp. 794–800. [CrossRef]
69. Chen, M.; Tang, X.; Cheng, J.; Xiong, N.; Li, J.; Fan, D. A DDoS Attack Defense Method Based on Blockchain for IoTs Devices. In Proceedings of the Communications in Computer and Information Science; Springer Science and Business Media Deutschland GmbH: Singapore, 2020; Volume 1253, pp. 685–694. [CrossRef]
70. Jia, B.; Liang, Y. Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain. *China Commun.* **2020**, *17*, 11–24. [CrossRef]
71. Rodrigues, B.; Scheid, E.; Killer, C.; Franco, M.; Stiller, B. Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks. *J. Netw. Syst. Manag.* **2020**, *28*, 953–989. [CrossRef]
72. Rodrigues, B.; Stiller, B. Cooperative Signaling of DDoS Attacks in a Blockchain-Based Network. In Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos, Beijing, China, 19–23 August 2019; pp. 39–41. [CrossRef]
73. Rodrigues, B.; Trendafilov, S.; Scheid, E.; Stiller, B. SC-FLARE: Cooperative DDoS Signaling Based on Smart Contracts. In Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020. [CrossRef]
74. Gruhler, A.; Rodrigues, B.; Stiller, B. A Reputation Scheme for a Blockchain-based Network Cooperative Defense. In Proceedings of the 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Arlington, VA, USA, 8–12 April 2019; pp. 71–79. Available online: https://ieeexplore.ieee.org/document/8717909 (accessed on 2 February 2021).
75. Killer, C.; Rodrigues, B.; Stiller, B. Security Management and Visualization in a Blockchain-Based Collaborative Defense. In Proceedings of the ICBC 2019—IEEE International Conference on Blockchain and Cryptocurrency, Seoul, Korea, 14–17 May 2019; pp. 108–111. [CrossRef]
76. Yeh, L.Y.; Lu, P.J.; Huang, S.H.; Huang, J.L. SOChain: A Privacy-Preserving DDoS Data Exchange Service over SOC Consortium Blockchain. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1487–1500. [CrossRef]
77. Pavlidis, A.; Dimolianis, M.; Giotis, K.; Anagnostou, L.; Kostopoulos, N.; Tsigkritis, T.; Kotinas, I.; Kalogeras, D.; Maglaris, V. Orchestrating DDoS mitigation via blockchain-based network provider collaborations. *Knowl. Eng. Rev.* **2020**, *35*. [CrossRef]
78. Purohit, S.; Calyam, P.; Wang, S.; Yempalla, R.K.; Varghese, J. DefenseChain: Consortium Blockchain for Cyber Threat Intelligence Sharing and Defense. In Proceedings of the 2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020; pp. 112–119. [CrossRef]
79. Yeh, L.Y.; Huang, J.L.; Yen, T.Y.; Hu, J.W. A Collaborative DDoS Defense Platform Based on Blockchain Technology. In Proceedings of the Proceedings—2019 12th International Conference on Ubi-Media Computing (Ubi-Media), Bali, Indonesia, 5–8 August 2019; pp. 1–6. [CrossRef]
80. Spathoulas, G.; Giachoudis, N.; Damiris, G.P.; Theodoridis, G. Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets. *Futur. Internet* **2019**, *11*, 226. [CrossRef]
81. Tukur, Y.M.; Thakker, D.; Awan, I.U. Ethereum Blockchain-Based Solution to Insider Threats on Perception Layer of IoT Systems. In Proceedings of the 2019 IEEE Global Conference on Internet of Things (GCIoT), Dubai, United Arab Emirates, 4–7 December 2019.