A survey on Blockchain solutions in DDoS attacks mitigation : techniques, open challenges and future directions

Rajasekhar Chaganti[a,*], Bharat Bhushan[b,*], Vinayakumar Ravi[c,*]

[a]*Dept. of Computer Science, University of Texas at San Antonio, San Antonio, Texas 78249, USA.*
[b]*Department of Computer Science and Engineering, Sharda University, India.*
[c]*Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar, Saudi Arabia.*

Abstract

With the proliferation of new technologies such as the Internet of Things (IoT) and Software-Defined Networking (SDN) in recent years, the Distributed Denial of Service (DDoS) attack vector has broadened and opened new opportunities for more sophisticated DDoS attacks on the targeted victims. The new attack vector includes unsecured and vulnerable IoT devices connected to the internet, and denial of service vulnerabilities like southbound channel saturation in the SDN architecture. Given the high-volume and pervasive nature of these attacks, it is beneficial for stakeholders to collaborate in detecting and mitigating the denial of service attacks promptly. Blockchain technology is considered to improve the security aspects owing to the decentralized design, secured distributed storage, and privacy. A thorough exploration and classification of blockchain techniques used for DDoS attack mitigation are not explored in the prior art. This paper reviews and categorizes state-of-the-art DDoS mitigation solutions based on blockchain technology. The DDoS mitigation techniques are classified based on the solution deployment location i.e. network-based, near attacker location, near victim location, and hybrid solutions in the network architecture with emphasis on the IoT and SDN architectures. Additionally, based on our study, the research challenges and future directions to implement the blockchain based DDoS mitigation solutions are discussed.

Keywords: Denial of service attack, IoT botnet, Software Defined Networks, Smart contract, Blockchain, DDoS attacks, Internet Service Provider

1. Introduction

In recent years, DDoS attacks has been growing, and have always seen an upward trend [1]. Work from home and increased use of cloud technologies owing to the Covid pandemic in the first quarter of 2020 have increased the volume and intensity of DDoS attacks in 2020. For example, launching various amplification and User Datagram Protocol UDP-based attacks to flood target networks increased 570 percent for the second quarter of 2020 in comparison with the previous year for the same time period [2]; the traditional threshold-based mitigation methods are insufficient to detect these attacks and the machine learning models can accurately detect as long as the attack pattern follows the trained data model and if any new attack pattern can easily evade these models [2]. Although the DDoS attack vectors have existed for years and many solutions have been proposed for handling the attacks, it is still an important problem to be addressed as the new technologies increase the attack surface and exploitable vulnerabilities.

As the number of devices connected to the internet increases and new network protocol vulnerabilities is uncovered, e.g., the UDP Memcached vulnerability [3], DDoS attack rates have increased exponentially over the last decade, as shown in Fig 1. For instance, the number of Mega millions of packets per second(Mpps) generated by the DDoS attacks exponentially increased from 2010 to 2020. A similar trend is followed for attack-generated traffic in bits/seconds, as seen in Fig1. A nominal enterprise organization may not be able to effectively handle or mitigate the current terabit rate-sized attacks, and it is already late to bring up the network Operators and internet service providers to react and mitigate DDoS attacks when attackers target these enterprises. However, as mentioned in Table 2, we can see that the cloud service providing organizations like Amazon Web Services (AWS) and Google Cloud Platform (GCP) handled approximately more than 2 Tbps attack rate at the edge level and served the public cloud application customers with no performance or service impact in the last two years. In 2016, the IoT devices such as routers and cameras connected to the internet were compromised, and attack code was deployed to launch Mirai bot reflection attacks to generate attack traffic rates in excess of 1 Tbps targeting DYN (a dynamic DNS service provider), OVH

*Corresponding author
Email addresses: Raj.chaganti2@gmail.com (Rajasekhar Chaganti), bharat_bhushan1989@yahoo.com (Bharat Bhushan), vravi@pmu.edu.sa (Vinayakumar Ravi)

(cloud service provider), and security blogger Brian Krebs's website [4] [5] [6][7].

The emerging technologies such as Cloud Computing, IoT, and SDN change the internet network architecture and offer new opportunities for the attackers to find the loopholes and perform Denial of service attacks. The challenge of large-scale DDoS attacks is to mitigate them quickly and avoid the loss of business and reputation for the enterprise organizations involved in the attack. Therefore, rapid coordination and response are required between the stakeholders like network operators, edge protection providers, Internet service providers, impacted organizations, third-party DDoS mitigation services, etc. Authenticating and establishing trust among the parties involved is essential to execute legitimate actions for stopping the attacks. A blockchain is a distributed ledger that can record transactions in an efficient and permanent way. It is managed by peer-to-peer (P2P) network nodes with standard protocols designed for internode communication to approve the transaction records and validate the blocks. Owing to the inherent security by design and unalterable transaction records in the chain of blocks, a blockchain can be used for many applications including finance, healthcare, supply chain, cryptocurrency, cybersecurity, smart contacts in particular validating the identity, providing the user anonymity [8]. The blockchain utility for cybersecurity applications has been growing with the demand to build secured systems and applications. The decentralized consortium blockchain implementation for industrial IoT [9] [10], credit based consensus mechanism for approving the transactions in industrial IoT [11] and implementing blockchain-based data storage and protection mechanism for defending the security attacks in IoT systems [12] [13] are some of the applications of the blockchain in IoT. Additionally, blockchain is leveraged for security in other areas like secured storage of the data in mobile ad hoc networks [14], decentralized DNS database for DNS attacks mitigation such as cache poisoning attacks [15], secured data storage in the cloud and defend against the keyword guessing attacks [16]. Furthermore, based on the blockchain exhibiting security properties, we could see the potential to utilize the blockchain for security threat information sharing among the key stakeholders.

Recently, a few researchers proposed blockchain based solutions for threat information sharing like malicious IP addresses for blocklist, identifying the IoT bots in the network at the network gateway level, enabling Content Distribution Network (CDN) nodes near the victim using private blockchain when denial of service is identified, security operating center threat sharing to users accessed in the private blockchain is investigated in several recent works [17] [18] [19] [20] [21]. But there is a knowledge gap between network security experts, who aim to mitigate DDoS attacks in real-time and blockchain experts, who develop decentralized applications but may not be experts in network attacks. Our prior art research shows no significant work investigating blockchain's role in mitigating DDoS attacks. Therefore, we perform a comprehensive review of blockchain technology to handle denial of service attacks. In addition, the blockchain based solutions are categorized based on the DDoS mitigation deployment location in the internet while discussing various technologies such as IoT, SDN, and machine learning involved in addressing the DDoS solutions. In the end, the main contributions of this paper are as follows:

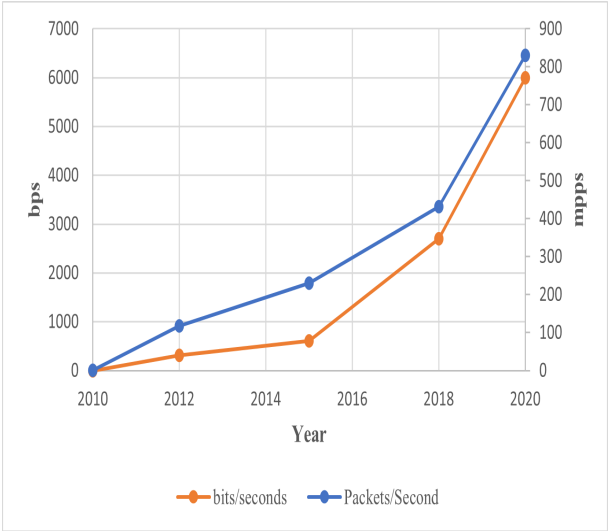

Figure 1: DDoS attack rate growth trend in the last decade.

- We performed a comprehensive review and classification of the role of blockchain technology in DDoS attack detection and blockchain-based DDoS mitigation solutions.
- We discussed the open challenges and future directions to implement and propose new solutions for handling DDoS attacks using blockchain.
- We categorized and described the existing blockchain related DDoS solutions based on the solution deployment location in the internet architecture.
- We discussed the blockchain based DDoS solutions leveraging the technologies IoT, SDN, and Machine Learning (ML) to address the DDoS attacks.
- Our findings show that secured collaboration among the stakeholders to share the DDoS threat indicators with blockchain is achievable while addressing the limitations.

In our work, we have conducted a survey of articles published in English over a period of the last six years (i.e., August 2016 to August 2022). As most blockchain-based DDoS mitigation schemes use Ethereum to store the network data as a transaction, and Ethereum was released in the middle of 2016, we have restricted the relevant article search from 2016.

Academic databases such as Google Scholar, ACM Digital Library, IEEEXplore, and ScienceDirect were used to run the search queries with the combinations of the following keywords such as "Blockchain", "Denial of Service", "botnet", "Ethereum", "Smart Contract", "DDoS", "Software-defined networks", "Internet of Things". The "blockchain" is a must keyword in all the searches. The relevant articles were shortlisted by reading the title and abstract of the retrieved search results. Overall, 84 relevant publications were identified during the prior art search process and used to perform our study on DDoS mitigation using Blockchain technology.

The abbreviations used in the paper are given in Table 1. The remainder of this paper is organized as follows: Section 2 discusses the key concepts such as DDoS attacks, Blockchains, and Emerging technology network architecture paradigms and related work in association with our topic in the paper. Section 3 describes our motivation for doing this work and the problem statement we are trying to address in the paper. Section 4 discusses the related work of using blockchain technology to handle DDoS attacks. Section 5 presents the Blockchain based solutions to mitigate the DDoS attacks. Section 6 depicts the future directions in accordance with advancements in Blockchain technology. Section 7 presents the current open challenges to utilize the blockchain in the context of DDoS attacks. Section 8 concludes the paper.

2. Key Concepts and Background

In this section, we review DDoS attack types, the solutions proposed to mitigate them, the main fundamentals and terminology of blockchain technology, and the emerging technologies such as the internet of things and software defined networking paradigm used to deploy the solutions or leverage to initiate the DDoS attacks. These are essential and play a significant role in understanding recent DDoS attack variants and their mitigation solutions using blockchain.

2.1. DDoS Attack Types and Known Solutions

DDoS Attack is a well-known and major concern in the cybersecurity area violating the security principle "Availability" of services. DDoS attack vectors exploit various features of the internet protocols, most of which were designed decades ago when security was not a concern. The relationship between an attacker exploiting the protocol features such as TCP connection setup using a three-way handshake and its victim is asymmetric in nature. DDoS attacks are mainly classified into two categories: bandwidth depletion and resource depletion attacks [28]. In the former attack, high traffic volumes that look legitimate but not intended for communication are directed to a victim. In the latter attack, the victim is inundated with bogus service requests that deplete its resources and prevent it from serving legitimate requests. Multiple bots (network nodes compromised and controlled by an attacker)

Table 1: List of Abbreviations used in the paper.

ACK	TCP Acknowledgement Flag
AMQP	Advanced Message Queuing Protocol
AMP	Asynchronous Messaging Protocol
API	Application Programming interface
AWS	Amazon Web Services
AS	Autonomous System
BFT	Byzantine Fault-Tolerant
BGP	Border Gateway Protocol
CDN	content distribution network
CoAP	Constrained Application Protocol
CIDS	Collaborative Intrusion Detection System
CLDAP	Connection-less Lightweight Directory Access
DDoS	Distributed Denial of Service
DNS	Domain Name System
DOTS	DDoS Open Threat Signaling
DoS	Denial of Service
DOS	Decentralized Oracle Service
DPOS	Delegated Proof of Stake
EVM	Ethereum Virtual Machine
GRE	Generic Routing Encapsulation
GCP	Google Cloud Services
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IoT	Internet of Things
IPFS	InterPlanetary File System
IP	Internet Protocol
ISP	Internet Service provider
KNN	k-nearest neighbor
LSTM	Long short-term memory
MLP	Multi-Layer Perceptron
ML	Machine learning
MQTT	Message Queuing Telemetry Transport
NDP	Neighbor Discovery Protocol
NTP	Network Time Protocol
OF	Open Flow
PBFT	Practical Byzantine fault tolerance
PCA	Principal component analysis
PoS	Proof of Stake
PoW	Proof of Work
PSH	TCP Push flag
P2P	Peer to Peer
P4	Programming protocol-independent packet processor
RAM	Random-access memory
SDN	Software Defined Network
RNN	Recurrent neural network
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operating Center
SYN	TCP Synchronization Flag
TCP	Transmission Control Protocol
SVM	Support Vector Machine
TX	Transaction
UDP	User Datagram Protocol
UTX	Unspent Transaction Unit
XMPP	Extensible Messaging and Presence Protocol

Table 2: Major DDoS attacks in the history

DDoS Attack	Year	Attack Type	Attack Rate	Duration	Amp Ratio	Protocols Involved	Impact
Six Banks [22]	2012	Brobot	60 Gbps	2 days	-	HTTP, HTTPS, DNS, TCP	Web Service Outage
Spamhaus [23]	2013	Reflection Attack	300 Gbps	-	Up to 100	DNS,TCP	Offline
Hongkong Central [24]	2014	Brobot,TCP SYN, HTTPS Flood	500Gbps	-	-	TCP,HTTPS	Minimal
Cloudflare [25]	2014	Reflection Attack	400 Gbps	-	Up to 206	NTP	No
Mirai Krebs [5]	2016	Mirai, TCPSYN, ACK, ACK+PSH	Krebs 620Gbps	2-7 days	-	TCP, GRE, HTTP	Krebs Offline
OVH [6]	2016	Mirai, TCPSYN, ACK, ACK+PSH	OVH 1.1 Tbps	2-7 days	-	TCP, GRE, HTTP	OVH minimal
Mirai Dyn [7]	2016	Mirai, Reflection	1.5Tbps	1 day	Up to 100	DNS	Internet Outage
Google Attack [26]	2017	Reflection	2.5 Tbps	6 months	6-70	CLDAP, DNS, SMTP	No
GitHub Attack [3]	2018	Memcached Reflection	1.35Tbps	20 min	51000	UDP	Service Outage
AWS Attack [27][18]	2020	Reflection Attack	2.3 Tbps	3 days	56 - 70	UDP, CLDAP	No

are often used to launch DDoS attacks. Direct attacks on a victim typically use flooding in which many packets are sent from multiple bots to the victim. The attack examples include TCP SYN floods, UDP floods, ICMP floods, and HTTP floods [29] [30] [31]. Another tactic used in DDoS attacks is amplification. In Amplification attacks, the attacker sends network requests to the victim network via Domain Name System (DNS) or network time protocol (NTP) servers. The sender IP address is spoofed as the victims address so that DNS or NTP responses send to the victim network. The DNS response bytes are several times larger than the DNS requests to the server. So, when all the network responses are sent to the victim network, the victim network is overwhelmed with the attack traffic and consumes all the victim network resources. Examples of amplification attacks include Smurf, Fraggle, SNMP, NTP, and DNS amplification [32] [30] [33][34].In addition, protocol exploitation attacks like TCP SYN flooding can be performed on the victim infrastructure by taking advantage of the TCP connection establishment mechanism. An attacker sends a flood of TCP SYN packets with no ACK responses to consuming the victim machine resources [35]. The adversary may also use automated scripts to send TCP flags ACK, PUSH, RST, and FIN packet floods to saturate the communication channel along with the victim infrastructure. Other categories of DDoS attack are ping of death and land attack. Ping of death attack focused on sending Ping command with packet size greater than maximum packet size 65536 bytes to crash the victim system. In land attack, An attacker may send forged packets with the same sender and destination IP address to target the victim to send the packet to itself forming an infinite loop and crashing the victim machine [35]. A zero-day vulnerability can also be leveraged to compromise the legit machines and successfully launch the denial of service attack [36].

Significant research work has been done on the detection and mitigation of DDoS attacks for the last two decades. The proposed mitigation solutions differ in the location and timing of deployment [37]. The deployment location-based solutions are categorized into four types

- Source-based defense implemented in the attack source edge routers or source Autonomous System(AS).
- Destination-based implemented at the victim edge routers or victim AS level.
- Network-based defense implemented by the Internet Service Provider(ISP) and core networks and usually required to respond to the attacks at the intermediate network level.
- Hybrid defense: the combination of the source, destination, and network-based mechanisms.

Although the source-based defenses aim to detect and mitigate the attacks in the early stages of the attack, it is very difficult to distinguish the legitimate and malicious DDoS traffic at the source level.

The destination-based defense mechanisms are easier and cheaper to implement since the attack traffic will be concentrated closer to the victim. However, before they are detected,

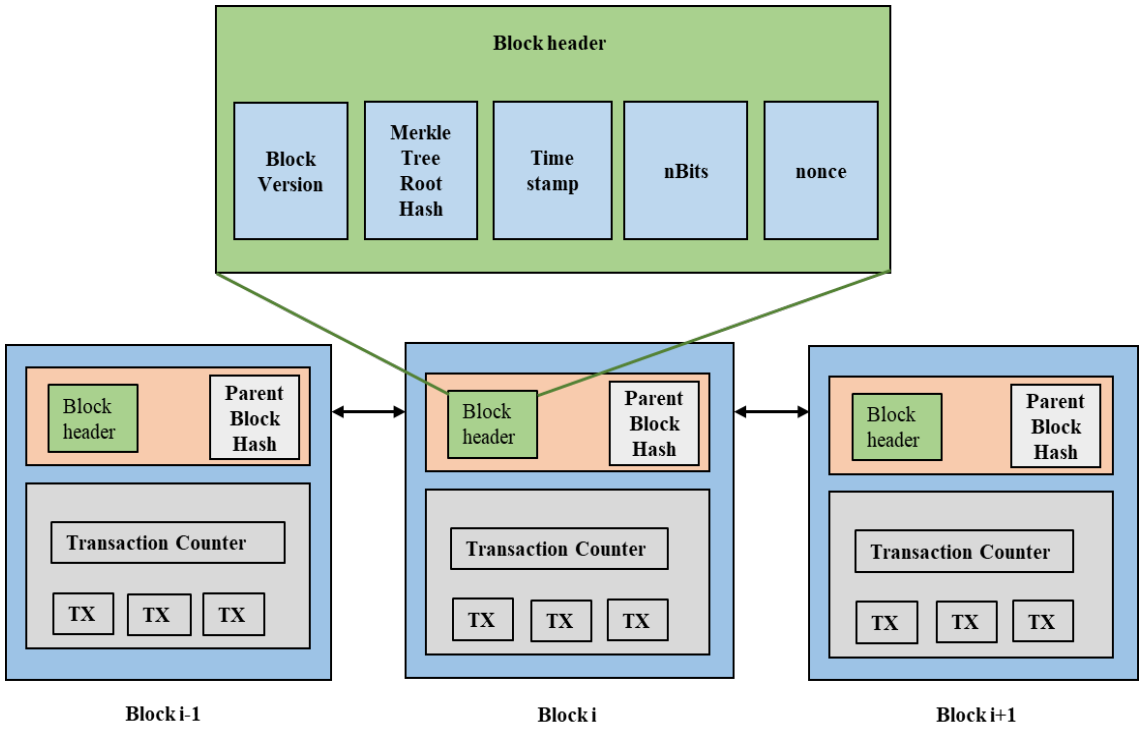

Figure 2: Blockchain Internal Components

the attack traffic consumes the resources on the paths leading to the victim. The network-based defense solutions detect and mitigate the DDoS attacks at the AS or ISP levels, which are closer to the attack sources. But they incur storage and processing overhead at the network infrastructure level, for example, by the edge or ISP routers, or might need additional DDoS protection devices like middleboxes to process the traffic. Also, the attack detection will be difficult owing to the lack of aggregation of traffic destined for the victim. However, attack mitigation in the internet core has the advantage of not passing the traffic to the victim network and preventing congestion of communication channels with attack network traffic, and saving the victim's computing and network resources. The hybrid defense approach promises to be more robust since it allows using a combination of defensive mechanisms to defend against DDoS attacks. Furthermore, detection and mitigation can be implemented more efficiently. For instance, the detection can occur at the destination or network level, and the mitigation technique can be applied near the source to handle the DDoS attacks effectively. However, its implementation is more challenging because it requires collaboration and cooperation between different entities to exchange attack information without receiving sufficient incentives for some participants like service providers [37]. There needs to be trust between the stakeholders, given that the service providers are diverse, and not easy to trust the entities.

For descriptions of various DDoS mitigation techniques such as anomaly or signature-based detection, machine learning algorithms to attack detection, scrubbing, rerouting, and filtering/blocking techniques, see Zargar et al. [37] and [38].

2.2. *Blockchain Technology and Their Types*

A blockchain is a digital, public ledger that records a list of transactions and maintains the integrity of the transactions by encrypting, validating, and permanently recording transactions [39]. Blockchain technology has emerged as a potential digital technology disrupting many areas, including the financial sector, security, data storage,the internet of things, and more. One of the best-known uses of blockchains is the design of cryptocurrencies such as Bitcoin [39, 39, 40].

A blockchain is typically managed by a peer-to-peer network. It uses a peer-to-peer protocol such as the Distributed Hash Table (DHT) for internode communication as well as validating new transactions. Fig 2 illustrates the typical structure of a block: a linked list of blocks with a header block. Each block comprises a set of transactions, a count of the transactions in the block, and a header. The block header includes the block version, which tells the current version of the block structure, a Merkle tree root hash to incorporate the uniqueness of the transaction set in the block by determining the final hash value achieved from all the transactions in the block.The root hash maintains the integrity between the transactions in the block. Therefore, the transactions are secured in a blockchain and cannot be tampered with. The block header also contains Timestamp, i.e. the time at which the block is created and it plays an important role in extending a

blockchain to record new transactions.The nBits field signifies the difficulty level that is being used for miner computations to add the transactions to the block. The nonce field represents a random number created by the creator of the block and can be used only once. The parent block hash is a cryptographic hash value of the parent block to maintain the integrity between the two consecutive blocks and maintain the non-tampered chain of blocks. A special data structure points to the most recent block in a chain. Using the back pointers other blocks in the chain can be accessed.

Blockchain exhibits properties like decentralization, persistency, anonymity, and auditability. The essential anonymity property is achieved using asymmetric cryptography like RSA algorithm and digital signature [41]. Each user has a private and public key pair for applying an asymmetric cryptography algorithm. The hash values obtained from the existing transactions will be utilized to get the digital signature and validate the user's authenticity. The user validation is a two-step process: signing and verification. Fig 3 shows the asymmetric cryptography, and digital signature calculation steps during the validation process [42]. The peer-to-peer blockchain system has no centralized node. It uses consensus algorithms, which typically require participating entities to win a computing challenge, authorize an entity to create the next block of verified transactions, and append to the exiting blockchain. As shown in the 3, The owner sends a transaction as a hash value to the next owner. The owner's hash value is determined from the previous transaction value in the blockchain and the next owner's public key value. The generated hash value is signed by the owner's private key to preserve the ownership.

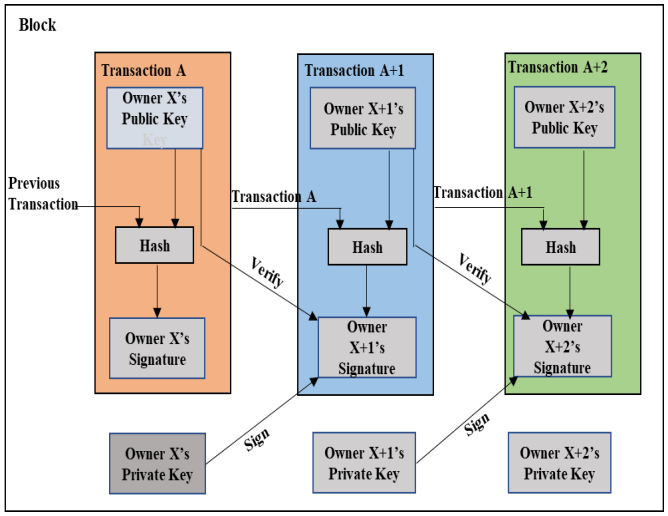

Figure 3: Basic cryptographic operations in blockchain .

A consensus algorithm, as indicated above, is used to select nodes in peer-to-peer blockchains to add a block of new transactions to the existing Blockchain. Some of the widely used algorithms are Proof of Work (POW), Proof of Stake (POS), Practical Byzantine Fault Tolerance (PBFT), ripple consensus algorithm, and delegated proof of stake (DPOS) [43]. In POW, used by Bitcoin, every node computes the hash value of the block header, and the computed value should be less than the specific value, according to the algorithm. The peer nodes will verify the success of the other nodes hash computations. The majority peer nodes approved node is selected as an authorized node to add the transaction to the block. This update is propagated to all other nodes of the Blockchain. Computation of the hash value within the constraints requires extensive computing, which is called as mining. In POS, users having higher stakes can get the authority to add the transactions in the Blockchain. So, richer entities will become richer, and a few participants will dominate the blockchain management and transaction approval. On the other hand, this method does not require extensive computing power and is likely to be more efficient. The consensus algorithm based on PBFT requires a significant majority of the nodes participating in the Blockchain should approve the transaction. The approved transactions to be appended in the network. PBFT tolerates 1/3rd of the node failures. The consensus process starts by choosing a primary node to process all the transactions in a block. It is a three-step process i.e., pre-prepare, prepare and commit; If 2/3rds of the nodes accept the request, then the transaction is appended to the block. Hyperledger Fabric is an example of using PBFT as a consensus mechanism to complete the transactions in the network. In DPOS, the delegated maximum currency stakeholder is chosen for adding the transactions. Some platforms like Tendermint operate on the combination of the algorithms (DPoS+PBFT) [43].

With decentralized consensus methods such as POW, and branching, the competing entities may propose different sets of transactions to create a new block and extend a current blockchain. It can occur due to the decentralized nature of mining to approve the transaction as well as having a delay to validate the 51% of the blockchain nodes or participants prior to adding the transaction to Blockchain. [43] [8].

In general, blockchain platforms are typically classified into three types. A public blockchain, in which anyone in public can read the existing transactions. But the transactions cannot be tampered with and provide high-level security, even though their computation delay is high. Bitcoin is a classic example of a public blockchain. Anyone can read the user account balance and the transactions that the user account involved, given the fact that the users bitcoin wallet address is known. In consortium Blockchain, only selected nodes have participated in transactional operations, and a good example is multiple organizations in a particular sector want to use the Blockchain for business applications. Each node represents a member of the organization. The consensus process is fast, and only privileged users can read the information from the Blockchain. Private Blockchain requires permission to join the network, and is usually maintained within the organization. The nodes can be the participants from the same organization to share the data within the organization, store the data

records securely, and more. The private Blockchain usually becomes centralized, and the transactions can be tampered if untrustworthy nodes participate in the mining process. The detailed comparison of the blockchain types is described in Table 3. The public blockchains are less efficient than Consortium and private based blockchains because the processing time for each transaction is high in the public blockchain. As the number of the nodes freely connected is more in the public blockchain, the transaction processing delay is higher in the public blockchain.

Since the existence of Bitcoin, the blockchain community has developed a number crypto coins focusing on specific industry applications. Some of the notable coins are Ethereum, Litecoin, and Ripple [44]. The second popular and largest market capitalization cryptocurrency is Ethereum, which works on smart contract functionality. Ethereum has been proposed to address some limitations in the Bitcoin scripting language. Ethereum supports the Turing complete programming language meaning that we can perform all computations, including the loops. The smart contracts run cryptographic rules when certain conditions are met. The smart contracts in the nodes are translated into EVM code, and then the nodes execute the code to complete the transaction (creating a user account, the result of code execution). The Ethereum network has scalability issues, and also their transaction fees are much higher[45]. To address these problems, Ethereum developers proposed Ethereum 2.0. Ethereum 2.0 works on the POS consensus mechanism to process the transactions and improve scalability. The first phase of Ethereum 2.0 launched in 2020. The full deployment of Ethereum 2.0 may improve the chances of wide adoption of the technology with low transactions fees.

There has been a lot of attention on Hyperledger recently owing to the applicability of its enterprise standard version capabilities. The Hyperledger is known to be used rigorously in academic research for validating the research claims and implementing applications in Blockchain. Hyperledger is an open-source community-contributed suite that comprises tools, frameworks, and libraries for enterprise blockchain application deployments. One notable tool is the Hyperledger Fabric [46], a distributed ledger user for developing blockchain applications and can have a private blockchain for serving the applications to specific services. The Fabric consists of a model file, script file, access file, and query file, and all zipped together to form a business network archive. The Fabric operates on "Chaincode," a similar concept to Ethereum smart contract for performing secured blockchain transactions. The distributed file storage, i.e., Interplanetary File System (IPFS), can also be attached to the Hyperledger Fabric. The IPFS stores the data and can be shared across the nodes in the blockchain. For example, a decentralized web application can be hosted with content stored in IPFS for serving web content to users. Overall, Hyperledger is a very useful platform for blockchain technology and has been widely used for developing applications, including DDoS mitigation.

2.3. Emerging Technology Network Architectures

Some notable recent technologies, such as IoT, SDN, and cloud computing, essentially changed the network paradigm. The Blockchain technology can only help to store the network records/DDoS threat intelligence information as a transaction in the ledger and distribute these transactions to the blockchain nodes located in remote networks to update the DDoS attack activity information and mitigate the DDoS attacks. The SDN and IoT networks are mainly leveraged to conduct DDoS attacks or implement DDoS mitigation solutions. The blockchain-based DDoS solutions are also integrated into the SDN or IoT networks to stop the attacks. So, it is essential to review these advanced network architectures to study the advanced DDoS attacks exploiting the architecture limitations and propose new solutions to mitigate these attacks using blockchain technology.

2.3.1. IoT Architecture

IoT is a system of computing devices, including the physical objects with network connectivity to the internet and transfer the data over the network with or without requiring human interaction. The tremendous progress toward smart homes, smart cities, smart transportation, and smart grid applications in recent years shows the rapid advancements in IoT technology. Gartner predicted that there will be 65 billion IoT devices connected to the internet by 2025.The current statistics show that around 31 billion IoT devices are deployed and connected to the internet [47].

Fig 4 depicts a typical IoT architecture with main components. The IoT devices can be sensors, actuators, or other appliances installed in homes, industries, human body, vehicles, or farming platforms to monitor or sense the current state or activity and pass the information to the nearest IoT gateway through wireless communication like Bluetooth, Wi-Fi, NFC, and ZigBee [48] [49]. The IoT gateways are connected to the public internet for sending the information to IoT service providers for data analytics, tracking the status, displaying in the user console, etc. They use IoT network protocols such as MQTT, AMP, HTTP, and CoAP but are not limited [50]. Due to the limited CPU, memory, and power capabilities of IoT devices and the multivendor IoT platforms, conventional security solutions are incompatible in the IoT environment. Securing the IoT devices with traditional network security solutions is a challenging task

2.3.2. SDN Architecture

Recent advances in wide area networks (WAN) and data center networks culminate the SDN paradigm. SDN logically enables centralized management of layer two and layer three devices such as Switches and Routers. It also includes the management of the organization's wide-area networks, where the network devices are located in multiple sites and

Table 3: Types of Blockchain and their Properties

Property	Public	Consortium	Private
Consensus participants	All mining nodes	Selected nodes	Nodes within the organization
Efficiency	Low	High	High
Readability	Anyone	Anyone or restricted members	Members within the organization
Decentralized(network)	Yes	Partial	No
Decentralized(blockchain)	Yes	Yes	Yes
Consensus authorization	Permissionless	Permissioned	Permissioned
Example	Bitcoin	R3	Hyperledger
Application	Bitcoin currency, voting	Banking, payments	Supply chain, health care, retail
Immutability	Nearly impossible to tamper	Possibly tampered	Possibly tampered

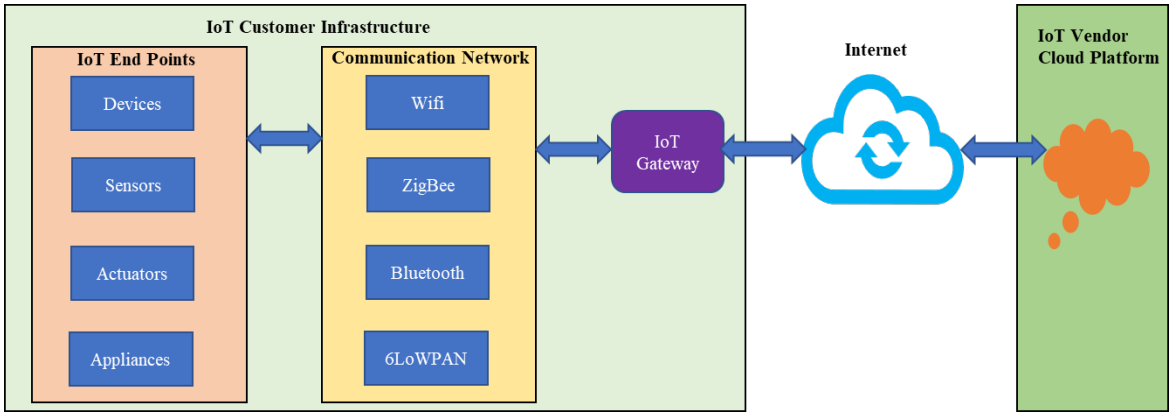

Figure 4: A typical IoT Architecture.

are monitored/controlled by an SDN controller [51]. As depicted in Fig 5, the central controller manage and monitor all the network devices in the data plane layer and communicate through southbound API like Openflow standard. The SDN controllers communicate with each other via westbound and eastbound API. The SDN controller may communicate with the SDN applications using northbound API when a network flow packet reaches the switch or routers in the data plane, the switch device searches in the lookup table for a match and then handles the packet by either sending it to the output port or dropping the packet. The packet will be forwarded to the SDN controller if the network flow packet does not find a match in the lookup table. The SDN controller updates the lookup table in the switches with action items and forwards the packet back to the switch. Now, the switch may forward the packet destination port.. A network administrator can develop the applications on top of the control layers to perform network management operations. SDN technology can be used at the autonomous system, internet service provider, or data center level for network monitoring and management. Although SDN has many advantages, including programmability, centralized control, and security, it also inherits security vulnerabilities due to the new architecture paradigm. For instance, an adversary may target the controller with a TCP SYN flooding attack and other protocol exploitation techniques to saturate the controller and shut down the whole network [52]. Leveraging the blockchain technology opens up new research possibilities to secure the Software-defined network itself from malicious denial of service attempts [53] as well as mitigation of the denial of service attacks in conventional networks. The Openflow protocol supports the communication between the network devices, and SDN controllers follow predefined Openflow protocol specifications. The Openflow protocol may not support the protocol processing customization, and the Openflow software is not independent of the underlying hardware specifications. So, the network domain-specific language Programmable protocol-independent packet processors (P4) is a network domain-specific language proposed to control the data plane devices in SDN [54]. The P4-enabled switches can be programmed to process customized protocol packets and support processing packets without relying on the device's underlying hardware support. The programmability and flexibility of operating the data plane with P4 in SDN have a good potential to implement network anomaly detection and mitigate the Denial of service attacks.

3. MOTIVATION AND PROBLEM STATEMENT

3.1. Motivation

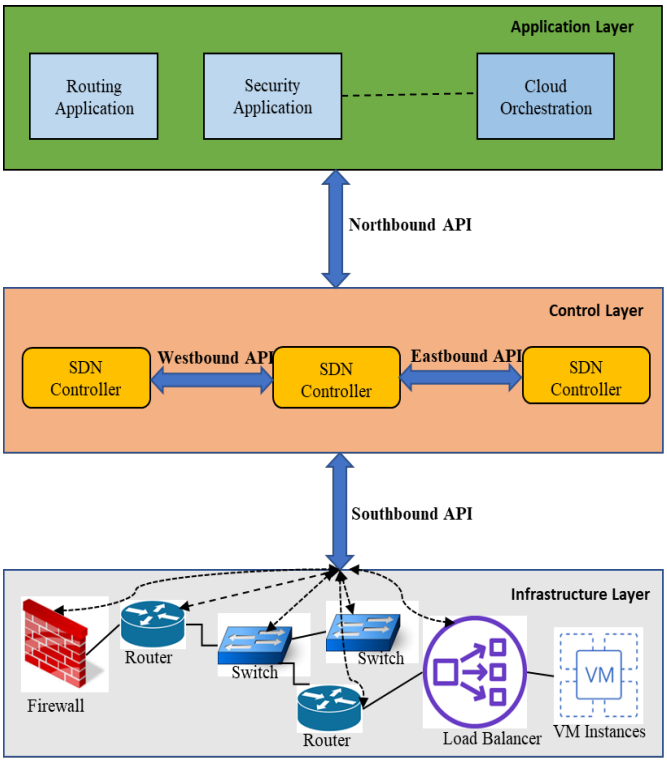

Figure 5: A typical SDN Architecture

Distributed denial of service attack is still a major threat to enterprises and large organizations. A successful denial of service attack can impact the customer's availability of resources. Availability is one of the fundamental requirements of the CIA triad security model. Most existing solutions monitor the DDoS attack traffic and reactively implement the attack mitigation solutions to block the attack traffic at various levels of the internet architecture. An effective DDoS solution is required to combat the attacks using advanced technological solutions. Blockchain technology has disrupted many fields like finance, supply chain, etc. Blockchain users are constantly exploring the application of blockchain technology in other fields. Blockchain properties like immutable transactions may be helpful to address DDoS attack detection and effectively mitigate the attacks. The malicious or rogue attacker IP addresses can be tracked and maintained within the blockchain distributed ledger. The distributed ledgers can be shared with interested stakeholders and enterprise security teams. Network security and Blockchain technology are two different technical areas. Little research has been done to propose new denial of service attack mitigation solutions. We are motivated to identify state-of-the-art DDoS attack mitigation solutions leveraging blockchain technology. We expect that our work will be considered a good reference for researchers to review the prior art solutions and propose new DDoS mitigation solutions using blockchain technology.

3.2. Problem Statement

The application of blockchain technology in solving DDoS attack detection and mitigation is hardly explored in the literature. The limited research is performed in the literature because of the lack of expertise in cross-domain technologies, little reference information available to the public, and the lack of research direction guidelines. The network security attacks like DDoS attacks are even more complex to understand and address with blockchain solutions, as the network architecture complexity increases with advancements in Software-defined networks and the Internet of things. So, understanding the various state-of-the-art blockchain-based solutions used to detect and mitigate DDoS attacks in complex network environments with IoT devices' presence and centralized network devices control is essential to progress the research in the right direction. We want to bridge this knowledge gap between network security researchers and the blockchain developing community and empower the researchers to review this article as a reference point to continue the research of using blockchain technology to address the network security problem.

4. RELATED WORK

The advancements in technologies such as ML, Blockchain, IoT, and SDN may improve the human life experience in the digital world. These technologies are also being used to implement the security solutions in the internet era. For example, network security monitoring can be improved by implementing security solutions in SDN controllers. The entire network can be monitored using an SDN controller. The Internet of things has numerous security applications, such as monitoring the physical environment and notifying the user when an anomaly or suspicious event occurs.

However, the IoT and SDN technologies also exhibit new security concerns and issues [62] [63] [64] [65][66][52][67][68][69][70]. Some researchers also used the combinations of these technologies to address security challenges ranging from malware analysis, Domain Name System (DNS) Security, to network security as well as privacy issues [71] [72] [73][74] [75]. Our focus in this paper is specific to DDoS-attack detection and mitigation techniques in conventional networks, software defined networks, cloud environments and internet of things [35] [73] [76] [77] [78] and the Blockchain solutions used to mitigate the DDoS attacks. Some of the non-blockchain known techniques in the literature include ML or Deep Learning (DL) based detection, anomaly-based detection, and signature-based detection in IoT, SDN, or conventional networks.

Table 4 presents the existing state-of-the-art Blockchain and non Blockchain based DDoS mitigation solution survey papers and also compares our work with the existing

Table 4: Comparison of the state-of-the art review in Blockchain based DDoS mitigation solutions

Authors	Blockchain Discussion	IoT based DDoS/BC Solutions	SDN based DDoS/BC Solutions	ML based DDoS/BC Solutions	Future Directions	Open Challenges	Location based Categorization
Manavi et al [55]	No	No	No	No	No	Yes*	Yes
Vishwa et al [56]	No	Yes*	Yes*	Yes*	No	Yes*	Yes*
Alzah et al [57]	No	No	Yes*	No	Yes*	Yes*	No
Bawany et al [58]	No	No	No	Yes*		Yes*	No
Shah et al [59]	Yes	Yes	No	No	Yes	No	No
Wani et al [60]	Yes	No	Yes	Yes	No	Yes*	No
Singh et al [61]	Yes	Yes	Yes	No	Yes*	No	No
Our Work	Yes	Yes	Yes	Yes	Yes	Yes	Yes

*- Partially mapped: non blockchain DDoS solutions

Blockchain-based DDoS attack mitigation solutions. manavi et al. [55] discussed the DDoS attacks and mitigation solutions survey and categorized the solutions according to source, destination, network, and hybrid-based mechanisms. However, the paper did not include the Blockchain based DDoS attack solutions in the survey. Vishwa et al. [56] performed an IoT-based DDoS mitigation solution survey to identify the security gaps in the IoT networks. The authors covered various technological solutions like SDN and Machine learning-based DDoS mitigation solutions in the IoT space. But, the paper's main focus was exploring the DDoS attack mitigation solutions IoT. The article did not describe the Blockchain based DDoS attack mitigation solutions. Alzahrani et al. [57] performed the DDoS attack mitigation solution survey focusing on Software Defined Networks. SDN is vulnerable to new denial of service attacks like Controller saturation attacks. But, the paper has not mentioned the Blockchain based DDoS mitigation solutions. Bawany et al. [58] surveyed machine learning based solutions to address the DDoS attack detection and mitigation problem. The authors reviewed various DDoS attacks, including flooding and protocol based solutions. However, none of the solutions are implemented using blockchain technology. Overall, all the above mentioned survey papers mainly describe the DDoS mitigation solutions using SDN, IoT, or Machine learning technologies.

Although blockchain mainly provides anonymity, privacy, and secured data storage, few researchers explored the applicability of blockchain technology in DDoS attack mitigation and threat intelligence information sharing to respond to the attacks quickly. Singh et al. [61] presented a survey of DDoS mitigation techniques using blockchain technology. The authors considered four blockchain-based DDoS mitigation approaches for comparison, highlighted the operation of these mitigation mechanisms, and assessed the practical applicability of these implementations [79] [80] [81][82]. However, the authors did not perform a comprehensive review and analysis to identify the current challenges and future directions. et al. [60] discussed the prior art DDoS mitigation solutions using blockchain by describing the methodology on how the relevant papers are collected and proposing the taxonomy based on the technologies like artificial intelligence, information sharing capability, and blockchain types. However, the article did not present a comprehensive review of the state-of-the-art work with location based DDoS solution classification. Shah et al. [59] performed a study on the Distributed denial of service attack detection in the IoT using Blockchain technology. The authors discussed various Blockchain solutions to handle the DDoS attack and classified the blockchain based solutions based on the distributed architecture, access management, traffic control, and Ethereum platform. However, their work only covered the existing solutions to combat DDoS attacks in the IoT space. Additionally, the paper does not discuss the blockchain solutions classification based on

the network location. Our motivation for this work is to perform a detailed review of the existing blockchain based DDoS attack mitigation solutions, which not only cover the solutions proposed in the conventional network but also in software-defined networks and the internet of things. We have also reviewed the machine learning and deep learning based solutions implemented in blockchain for DDoS mitigation.

5. DDoS Attacks Mitigation using Blockchain

This section presents the existing research on addressing the DDoS attack detection and mitigation problem using blockchain technology. In addition to blockchain-based solutions, technologies such as SDN, IoT, and ML are discussed while addressing the DDoS attacks near the attacker domain location, the internet core, or the victim network domain.

Fig 6 represents a typical network level DDoS mitigation solution using blockchain technology architecture. An attacker may send the traffic from the source AS. The victim host resides in the destination AS. The intermediate AS forwards the network traffic from source AS to Destination AS or destination AS to source AS. An SDN controller controls all the network devices in the AS to ease network management and administration. The SDN and IoT infrastructure are typically part of the internet network architecture. Hence, we have discussed in detail these technologies for the reader's understanding of them when describing blockchain-based DDoS solutions. As shown in Fig 6, Ethereum nodes are installed on the SDN controller in each AS. The Ethereum node client invokes a smart contract to report the malicious or suspicious IP address when the malicious IP address is identified in the destination AS. The Ethereum node is updated with the suspect IP address in the destination AS. This event triggers a rule update in all the peer Ethereum nodes in the ASs, including the source AS and intermediate AS. Now, the controller reads the updated rule and pushes the rule to all the network devices such as switches and routers in the AS. When the adversary sends attack traffic to the victim device located in the destination AS, the network devices block the attack traffic at the source AS or intermediate AS level. In this way, blockchain technology is used to mitigate DDoS attacks with little human intervention effectively.

The advantage of blockchain based DDoS mitigation is the ability to block the attack traffic in the source domain. Blockchain-based solutions also reduce the cost of forwarding traffic across the core network and protect the core network from amplified attack traffic. Blockchain helps the security teams in an organization to securely share threat information such as malicious DDoS IP addresses across the security community, assuming that all the security members are part of the blockchain network. The effective sharing of the threat information helps organizations spontaneously respond to security attacks and improve the mean time to detection and mean time to remediation metrics. Furthermore, the

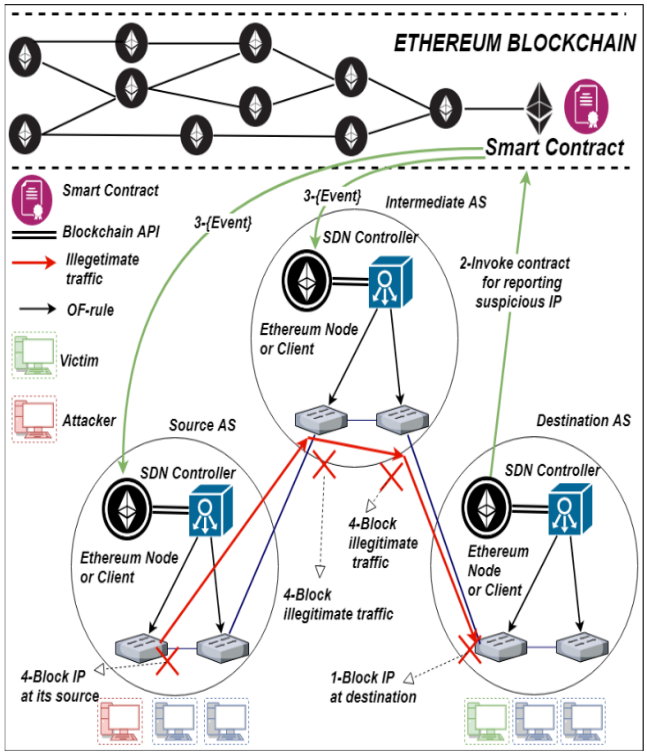

Figure 6: A typical Blockchain based DDoS mitigation

malicious IP records stored in the blockchain transactions are permanent, and an adversary will not be able to tamper the threat indicators stored in the distributed ledger. On the other hand, an adversary may compromise the organization's assets and even tamper the threat information stored in databases if the database systems are not hardened enough. But, the blockchain based DDoS attack may also have limitations. For example, the malicious IP addresses added to the ledger will not be removed from the blockchain. If an adversary spoofs the IP address with the legitimate user's IP address, the legitimate user will be blocked permanently and unable to access the internet.

Table 6 presents the categorization of the relevant papers with columns representing the paper objective, blockchain technology applied to mitigate the DDoS attacks, the advantage of the author's proposed approach, and the limitation of their work. We discuss and classify the existing DDoS mitigation blockchain solutions based on the location of solution deployment in the internet architecture. The network-level mitigation solutions include the solutions proposed at the ISP level, in which the ISP owns more than one autonomous system. The DDoS mitigation solutions proposed in the core backbone Internet network are also categorized under network-level mitigation solutions. The Near attack domain location-based solutions include the techniques proposed at the IoT gateway level when the attack originates from IoT devices. The attack originating AS based solutions, where

the AS owner (organizations or any entity) owns only that one AS are also categorized under near attack location based solutions. The near victim-based solutions include the DDoS mitigation solutions deployed in the victim AS network.

5.1. Network level mitigation

The network-level mitigation DDoS mitigation schemes using blockchain technology are deployed at the ISP level or the internet backbone core network, which may be far from an attacker or victims AS location. Table 6 illustrates the blockchain key concepts and technologies involved in the research works proposed for DDoS mitigation using blockchain. Table 6 clearly indicates that a smart contract based Ethereum network is mostly used for implementing the DDoS mitigation solutions in previous contributions, as shown in Table 5.

Tayyab et al. [83] proposed that each Intrusion detection system (IDS) in the network acts as a blockchain node and collaborates with other blockchain IDS nodes to share the attack information like correlated alarms. This decentralized correlated information sharing is used to detect ICMP6-based DDoS attacks. Although IDS collaboration improves DDoS attack detection capabilities, the practical implementation of IDS node collaboration may have difficulties. For example, the IDS vendor interoperability to support the blockchain technology is needed in an enterprise environment. Denial of service attacks detection at the IDS level is too late and might already congest the edge network communication channels or the content delivery network communications.

The following papers [20] [84] [85][86] [87] [88] [85] [82] [89] [80] [79] [17] focused on utilizing the SDN and blockchain technologies at the AS level to detect the denial of service attempts and activating the DDoS mitigation mechanisms at the network level. According to the authors proposed architecture, the autonomous systems consist of the SDN architecture, controlled by an SDN controller. The core concept in these papers includes leveraging the SDN's centralized controller application to update the network device's attack traffic actions rules. The usual action rules may be whitelisting or blocklisting the malicious IP addresses on the network devices.. The SDN controller node also acts as a blockchain node running decentralized application like Ethereum to store or validate the attack IP address list, and their blocklist/whitelist status as a transaction in the blockchain, and distribute the added transactions to all the nodes (SDN controller in other autonomous systems) in the blockchain. Ethereum smart contracts were used to store the IP addresses along with malicious flag status as a transaction. The DDoS detection/mitigation mechanism was tested in the Ethereum testing platform Rapsten testing network and also used Ganache for testing in local blockchain network [90].

Yeh et al. [20], Yeh et al. [86], Shafi et al. [93], and Hajizadeh et al. [91] discussed the threat information sharing including the DDoS threat data secure sharing among the collaborators using blockchain based smart contracts technology and decentralized data storage. The security operation centers can upload the threat data, and the ISP acts as a verifier to confirm the illegitimacy of the threat data before adding the transaction in the blockchain. The Ethereum based smart contract implementation for DDoS data sharing is performed for evaluation [20], [86] . But, in [91] and [93], the Hyperledger caliper is used to implement the threat information sharing among the organizations. Each organization may have the SDN controller to run the blockchain application and act as a blockchain node for updating the threat information in peer nodes.

Rodrigues et al. [89] [79] [17] proposed the Ethereum based architecture for DDoS mitigation and their hardware implementation to allow or block the malicious IP addresses in the ISP level. Each transaction may include the IP address and its status to detect the malicious IP address performing the denial of service attacks. The main limitation of the IP address data storage in the transactions may have limitations. But, Burger et al. [80] discussed that Ethereum is not an ideal technology for DDoS attack IP based signaling using blockchain due to the scalability issue. The authors also mention that Ethereum smart contracts can apply to a small number of IP address space related applications. They recommend storing the list of IP addresses in file storage like IPFS, the URL of the storage location pointing to the blockchain transactions, and the location integrity is verified using the hash value.

Pavlidis et al. [84] proposed a blockchain based network provider collaboration for DDoS mitigation. The ASs are selected based on their reputation scores to participate in the DDoS mitigation plan. The programmable data planes were used to implement the mitigation mechanism for DDoS attacks. This is in contrast to most of the works used the SDN Openflow protocol for network devices and SDN controller communication.

In the papers [95] [87], the machine learning algorithms such as K-nearest neighbors (KNN), decision tree, and random forest as well as deep learning techniques long short-term memory (LSTM) are applied to the network traffic to determine the DDoS attack. The papers also considered blockchain technology to whitelist/blocklist the IP addresses at the autonomous system level of the network. But, the application of machine learning on the network traffic requires infrastructure and computation capabilities, and ownership responsibility to allocate the resources. Any entity like ISP or security service provider will not be interested in performing data analytics unless they have any monetary benefits or

Table 5: DDoS mitigation near network using Blockchain

Title	Blockchain	Type	Consensus	Technologies
Yeh et al. [20]	Ethereum	Consortium	Proof of Work	Smart contracts, Swarm, DOS, Bloom filter
Yang et al. [88]	Ethereum	Permission	Proof of work	Smart Contract
Yeh et al. [86]	Ethereum	Consortium	Proof of work	Smart contract, Swarm, Oracle
Rodrigues et al. [89]	Ethereum	Public	Proof of Work	Smart Contract, SDN and VNF.
Burger et al. [80]	Ethereum	Public	Proof of Work	Smart Contract, Bloom filter
Rodrigues et al. [79]	Ethereum	Public	Proof of Work	SmartContract, SDN
Rodrigues et al. [17]	Ethereum	Consortium	Proof of Work	Smart Contract, IPFS, SDN
Hajizadeh et al. [91]	Hyperledger Fabric	Private	Kafka	Chain code, SDN, Threat Platform
Essaid et al. [87]	Ethereum	Public	Proof of work	Smart Contract, LSTM, SDN
Aujla et al. [92]	Generic	Private	-	SDN
Shafi et al. [93]	Hyperledger	-	Kafka	SDN, IoT
Pavlidis et al. [84]	Ethereum	Public, Private	Proof-of-Authority	Smart Contract
Abou et al. [85]	Ethereum	Public	Proof of work	Smart Contract, SDN

business advantage. These challenges need to be addressed to adopt the machine learning solutions along with blockchain based DDoS mitigation.

Most network-level solutions leverage the Ethereum blockchain network to implement the DDoS mitigation solutions. Ethereum blockchain seems to be chosen because of its wide adoption in the blockchain community, the development tools exist in public with great support from the community and the Ethereum currency is one of the accepted currencies in the blockchain industry. Overall, we can see that the combination of SDN at AS level and Ethereum smart contract can be implemented to track the IP addresses status and update all the nodes across the internet to mitigate the DDoS attacks. However, there are some limitations like blockchain integration with legacy networks, and handling spoofed IP addresses need to be solved for adopting the blockchain based DDoS mitigation at the network level.

5.2. *Near attack domain location*

The DDoS attacks mitigation at the attacker network is an effective way to handle DDoS attacks, as the attack traffic will not be propagated to the internet network. Most of the latest DDoS botnets are formed by compromising the legitimate IoT devices located all over the internet and targeting the victims to send malicious network traffic. So, detection and mitigation of IoT botnets at the source network is essential. We also categorize the AS based solutions under the near attack based category if the ISP owns a single AS and sends the attack traffic to the internet. For example, Abou et al. [85] is included in this category based on the ISP owning single AS and the attacker initiates the traffic from the same AS. Table 8 presents the advantage and the limitations of the existing near attack location blockchain based solutions.

Chen et al. [96] focused on detecting and mitigating IoT based DDoS attacks or botnets in an IoT environment using blockchain. The edge devices or IoT gateways act as a blockchain node to perform transactions when a network anomaly or attack is detected in the IoT environment. The techniques used for network traffic analysis in the paper include statistical analysis, and conventional bot detection techniques like community detection. The smart contracts are used to write attack alert data in transactions and the Ethereum network distributes the data across the IoT nodes. But, the IoT gateway nodes are not usually customer-centric, and deploying the blockchain client application in the gateway is challenging for a real-time production environment.

Javaid et al. [81] discussed the blockchain-based DDoS attack detection on the servers connected to the IoT devices. The Ethereum network approves the IoT devices sending data to the server at the expense of gas cost. When a rogue IoT device tries to send the malicious network traffic, the IoT device is penalized with high gas cost, and only trusted devices are approved for connecting to the network. The integration of the IoT with Ethereum enables the denial of service mitigation on the IoT device-connected servers. Sagirlar et al. [97] proposed a blockchain solution for detecting the IoT-related peer-to-peer botnets. The assumption is that botnets frequently communicate with each other to perform malicious activity. The authors mentioned that the network traffic between the botnet nodes is considered as blockchain transactions in permissioned BFT and use these transactions to identify the botnet IoT devices. The proposed method may not be viable, as the network traffic flows are enormous, and the blockchain may not accommodate the transaction capacity needed for storing in blockchain nodes.

Spathoulas et al. [98] presented an outbound network

Table 6: Advantages and limitations of near network based Blockchain solutions

Title	Objective	Advantage	Limitations
Yeh et al. [20]	Decentralized DDoS info sharing	SOC may use DDoS data among peers	Selecting the data certifier is challenging
Yang et al. [88]	Blockchain based DDoS mitigation services	Client validation and provider authentication	Spoofed IPs are ignored
Yeh et al. [86]	Collaborative DDoS info sharing	SOC info share platform	Spoofed IPs are ignored
Rodrigues et al. [89]	Blockchain based DDoS mitigation architecture	First architecture proposal in Blockchain based DDoS mitigation	Spoofed IPs are ignored
Burger et al. [80]	Scalable Ethereum based DDoS detection	Practical implementation	Questions on Ethereum usage
Rodrigues et al. [79]	Blockchain architecture and design for DDoS	Detection and mitigation also included	not for spoofed IP
Rodrigues et al. [17]	Ethereum testbed for DDoS mitigation	Tested on hardware	Scalability
Hajizadeh et al. [91]	Blockchain based threat intelligent platform	Important security application	Fault tolerance
Shafi et al. [93]	Mitigate the IoT based DDoS attempts in SDN	-	Not support for non-SDN
Essaid et al. [87]	DL and smart contract DDoS detection	DL based solution	Standard dataset
Pavlidis et al. [84]	collaborative DDoS mitigation at the AS level	Network level DDoS mitigation	Difficult to identify slow DDoS attacks
Abou et al. [94]	Intra-domain and inter-domain DDoS mitigation	Effective DDoS mitigation	Spoofed IPs are ignored

traffic sharing among the blockchain-enabled IoT gateways to detect the IoT botnet. The authors performed simulations on the proposed solution and showed promising results using the detection efficiency parameter. But, the solution is not tested in the real blockchain nodes installed in the gateway, and mentioned that Ethereum smart implementation is one of their future work. But, in general, the IoT gateways are multivendor devices, and interoperability among the devices is an issue.

Abou et al. [85] discussed collaboration among autonomous systems to detect DDoS attacks. Each AS contains an SDN controller, in which blockchain application like Ethereum client is installed to distribute the malicious IP addresses among other ASs. Whenever a malicious IP address is identified in the AS, the SDN controller updates the Ethereum client in the ASs for DDoS detection and mitigation. To implement this solution, the ASs should support the same SDN controller and agree to work for DDoS mitigation collaboratively. Kataoka et al. [82] presented a similar [85] blockchain and SDN based architecture for whitelisting the IoT devices in the network. The trusted profile consists of IoT devices will be stored in a smart contract based blockchain transaction, and the SDN controller will update all the switches and routers in the SDN network. This implementation enables the malicious or IoT botnets to be blocked in the attack network and protect the networks. Considering a huge number of IoT devices connected to the internet, approximately 31 billion devices as of 2020, implementing the blockchain for each gateway in the IoT environment is challenging and practically impossible. In addition, the IoT gateway vendors interoperability and supporting the blockchain nodes just for the sake of DDoS detection and mitigation may not seem reasonable with the current state-of-the-art technology.

The authors in [99] proposed a smart contract based collaborative IoT botnet mechanism. The smart contract is updated with the botnet device information, including the IP addresses, whenever an IoT botnet is identified. The stakeholders in the blockchain can read the updated smart contract and can implement the mitigation rules in their network devices to block the IoT botnet traffic. Jiang et al. [100] proposed a blockchain based solution to prevent SDN-based DDoS attacks. The attack traffic record is updated in the blockchain node connected to the SDN controller. The attack information is updated to all the other SDN controllers in other Autonomous systems via blockchain nodes to block the attack traffic. The authors [101] presented a multi-level DDoS mitigation solution using blockchain in IoT environments. Ac-

Table 7: DDoS mitigation near attack location using Blockchain.

Title	Blockchain	Type	Consensus	Technologies
Chen et al. [96]	Ethereum	Public	Proof of work	Smart contract, IOT
Javaud et al. [81]	Ethereum	Public	Proof of work	Smart Contract, IoT
Sagirlar et al. [97]	Hyperledger (Future work)	permission	BFT	IoT, Chaincode
Spathoulas et al. [98]	Ethereum (Future work)	Public	Proof of work	IoT, Smart Contract
Abou et al. [85]	Ethereum	Permission	Proof of work	SDN, IOT
Kataoka et al. [82]	Ethereum	Public, Private	Proof of work	Smart Contract, SDN, IoT
Sajjad et al. [99]	Ethereum	Public	PoW	Smart Contract, IoT
Jiang et al. [100]	Ethereum	Consortium	PoW	Smart Contract, SDN
hayat et al. [101]	Hyperledger	Consortium	BFT	Smart Contract, IoT

cording to the authors, the blockchain is used to verify the attack on the IoT device. If the IoT device is identified as malicious, the IoT device is excluded from the IoT network to prevent attacks. Overall, selecting the accurate DDoS attack information (IoT device, IP address, MAC address) to share with other nodes is very important in the proposed methods, as the network architecture and security control implementation is different in SDN and IoT infrastructure.

5.3. Near Victim Location

Yang et al. [88] proposed a real-time DDoS mitigation service leveraging a consortium based or permissioned blockchain. Each DDoS service provider has an account in the permission blockchain to provide a DDoS mitigation service. The victim looks for the attackers IP-AS mapping in the blockchain, and the trusted service provider IP tagged with AS is authorized to provide the DDoS mitigation service. The authors also proposed the reputation or credibility validation mechanism for the service providers. However, if the attacking IP is spoofed, the authors proposed blockchain based DDoS mitigation service is not applicable. Kyoungmin Kim et al. [18] proposed a decentralized CDN service to mitigate the DDoS attacks with the help of a private blockchain and is mainly used by government and military agencies to protect their service. The victims are usually the service providers hosting the web content servers, and they can protect the servers using the decentralized CDN services.

The context of the attacker and victim location may be changed based on the attack type and how the attack is conducted. For example, an attacker may use their infrastructure to send the malicious traffic. In this case, the blockchain based solutions proposed in the attacker domain can be considered as near attacker-based solutions. Also, if the attacker compromises the legitimate IoT devices and uses them as a botnet to attack another victim. Here, the solutions deployed in the IoT device locations also categorized under near attacker location based solutions. The solutions implemented solely in the main victim (not the IoT compromised bot devices owner) network are categorized in the Near victim location-based solutions. Overall, we conclude that near the victim based solution research articles are very few than the network-based and near attacker based solutions. It is too late to mitigate the DDoS attacks near the victim. So, the existing solutions mainly focused on the network level or near attacker.

5.4. Hybrid solutions

The hybrid DDoS detection and mitigation solution can be the combination of the network based, near attacker location, and the near victim location based solution. For effective mitigation of the DDoS attacks, multi level mitigation solutions are needed. But, the implementation of these solutions requires collaboration among stakeholders. Abou et al. [94] proposed intra domain and inter domain DDoS detection and mitigation solutions using blockchain. The intra-domain detection includes near victim based solutions and inter domain detection, meaning that network based solutions. The Ethereum smart contract is deployed in each AS to distribute the DDoS threat information. The SDN controller is used to update the AS network traffic filtering rule to block the malicious traffic for inter domain DDoS mitigation. On the other hand, the traffic from switches and routers in the same domain is monitored using SDN controller applications. The flow control rules are applied in switches/routers using the open flow switch protocol. This mechanism mitigates the internal attacks originating from the same domain. The hybrid blockchain based DDoS mitigation solutions may help effectively mitigate the attacks. Based on our research, there is little work on proposing solutions in multi-level internet architecture. The reasons may be a lack of expertise in more than one area, and the researchers may not yet explore blockchain-based hybrid solutions. Our survey analysis indicates that there is a scope to propose new hybrid solutions using blockchain and progress the research to use blockchain for DDoS attacks mitigation.

Table 8: Advantages and limitations of near attack location based blockchain solutions

Title	Objective	Advantage	Limitations
Chen et al. [96]	IoT based DDoS detection using blockchain	The Attacks can be stopped at the source network	Practically may not be viable
Javaid et al. [81]	Ethereum and IoT integration for DDoS	Automated control of the server IoT inbound traffic	Only applicable to server DDoS
Sagirlar et al. [97]	IoT botnet detection using BFT.	First blockchain-based IoT botnet detection	May not be scalable
Spathoulas et al. [98]	IoT botnets detection using blockchain	Outbound traffic exchange using IOT gateway	Not practically implemented
Abou et al. [85]	AS level SDN and blockchain solution	Network level DDoS detection	AS legacy networks issue
Kataoka et al. [82]	IoT botnets detection using SDN and blockchain	Attacker location based detection	Not applicable to non SDN based IoT
Sajjad et al. [99]	IoT botnets mitigation using blockchain based collaboration	Proactive attack mitigation	IoT devices not capable of running blockchain functionality
Jiang et al. [100]	mitigation of SDN based DDoS attacks using SDN	forged attack traffic discarded at the source switch	limited to SDN based DDoS attack prevention only
hayat et al. [101]	IoT device based attack verification mechanism using blockchain	Exclusion of malicious IoT devices from the network	IoT devices are resource constraint

6. Future Directions

In this section, the future directions of dealing with DDoS attacks using blockchain technology are explored. We have presented the research directions regarding the advancements in Blockchain and how these advancements can be used to address the DDoS attacks.

6.1. Internet of Blockchain

The current blockchain technologies like Bitcoin or Ethereum smart contracts transaction process is sequential; hence, adding the transactions in the Blockchain is very slow. To solve the scalability and interoperability issue between blockchain nodes, internet connected Blockchain has been proposed and can concurrently process the transactions from different blockchains. Paralism [102] built the blockchain infrastructure with unlimited scalability and a digital economy platform supported by parallel Blockchain. Customized script and chain virtualization make parallelism support any amount of sub-chains and independently operated chain-based applications and also become the backbone of the internet in a decentralized world. This technology is in the early stages of development and there are a lot of scopes to work on utilizing parallel Blockchain to share the threat data across the blockchain applications and protect against denial of service attacks. We also think that the parallel Blockchain surfaces new security issues, including leaking the information between the blockchain applications and will be the topic to focus for researchers while building the blockchain internet backbone. Another notable advancement in the Blockchain is Xrouter, which acts as a blockchain router to communicate one Blockchain-like bitcoin to smart contracts, supporting interchain and multichain services [103].

6.2. Programmable data planes (P4) for Blockchain based DDoS Solutions

The network paradigms keep changing as new technology trends emerge in the enterprises. The Internet of Things supports IP and IoT application protocols MQTT, XMPP, AMQP, etc. The denial of service attacks can be carried out by leveraging the weaknesses in the protocol and flooding the traffic on the victim machine. The combination of Programmable data planes at the gateway level and the blockchain technology for sharing the attack data is effective for mitigating the attacks. The P4 device in the switch level can parse any type of network protocol and makes it easy to apply blockchain technology. We envision that the future work would be proposing new architecture with P4 for mitigation of attacks, and developing smart contracts for the gateway level device to monitor and mitigate the attacks using Programmable data planes.

6.3. Threat Information Sharing using Blockchain

Consortium or private based blockchains are most compatible for sharing the threat information among the Blockchain participants. Numerous Ethereum based techniques has applied to share the information with integrity and anonymity. Leveraging the decentralized file storage such as swarm, IPFS enables to store of the information rather than keeping the data in transactions and causing time delay to process the sequential transactions. We believe that the information-sharing

field using Blockchain requires improvement and architecture changes to implement a secured information-sharing network.

6.4. Ethereum 2.0 Network for DDoS mitigation

DDoS solutions implemented using Ethereum network [86] [85]faces scalability, speed challenges, in particular, transactions refer to allow or block attack IP addresses. Ethereum 2.0 has been proposed and implemented for the last few years [45]. From August 2020, the upgradation to Ethereum 2.0 is initiated with three phases to complete the process. ETH 2.0 works-based POS rather than POW, which is a major change and the upgradation supports the drastic increase in network bandwidth, Lower Gas Costs, and benefit for scalability of the network. We envision implementing the DDoS mitigation scheme in Ethereum 2.0 in the near future.

6.5. Denial of Service attacks detection in Blockchain

Although the decentralized blockchain application is fundamentally secured, they are prone to denial of service attacks. A successful denial of service attack in Blockchain financial applications can have a significant financial loss to the stakeholders. For example, if an adversary controls 51% of nodes, then the typical user will not be able complete the transactions [104]. It may lead to denial of service attacks in the blockchain. The other types of attacks include eclipse attacks [105], mem flood attacks [106], or zero-day vulnerabilities in the applications code resulting in a denial of service attacks in the blockchain. One of our future work will be identifying all the denial of service attacks in blockchain technology and proposing novel solutions to mitigate the attacks in the blockchain.

7. Open Challenges

In this section, we discuss the research challenges to leveraging the blockchain technology for DDoS attack detection and mitigation solutions. The detailed description of the decentralized technologies adoption in conventional network issues is presented to handle the DDoS attacks.

7.1. Integration with Legacy Network

Distributed denial of service attacks mitigation involves the network operators, internet service providers, and edge network service providers to respond and block the malicious actor traffic. These stakeholders run the network services in legacy platforms, and have been providing services for decades, and adapting to the decentralized blockchain technology is a major concern. The reasons could be the lack of memory and computation requirements for blockchain in legacy networks [91], trust in the technology, unavailability of blockchain professional workforce, and fear of failure to protect customers while using blockchain. In addition, a collaboration between the ISPs is required to share the malicious data indicators among the ISP, and all the stakeholders may not be comfortable, as there is no monetization aspect for the internet service providers and usually only benefited by the attack victims. So, a responsible organization or service provider should be stepped up to coordinate among the stakeholders and ensure the involved stakeholders benefit.

7.2. Bitcoin/Ethereum P2P Network Zero-Day Vulnerabilities

The Blockchain transactions process includes the network traffic passing through the internet from one node and other nodes in the network; the cryptocurrency exchanges can also act as a blockchain node on behalf of the client and perform the transactions in the exchange conventional network. The attack vector for the blockchain is relatively broader, and the cost of a single vulnerability in the applications is millions of dollars. For instance, a parity check vulnerability in Ethereum causes lost $300 million dollars [107] and a small bug found in cryptocurrencies has a significant impact on the decentralized network. It is also important to note that the cryptocurrency exchanges having conventional networks will significantly impact the P2P applications. We envision that there is a scope to progress for developing flawless applications and monitoring the traffic for illegitimate activity detection.

7.3. Lack of Blockchain P2P Network Datasets

Monitoring the anomalous behavior of the blockchain network traffic and transactions dataset using machine learning and deep learning techniques is one of the solutions for detecting the DDoS attacks proposed in the prior art [83] [70]. But very few public datasets are available for continuing research and improving the detection metrics. Mt.Gox exchange trading activity data from 2011 to 2013 is available for the public to use for research purposes [108]. The quality of the data and how older the data are questionable for testing and detecting real-time attacks. We believe that having standard datasets and the application of big data analytics in the future is a must requirement for research progress in DDoS detection in cryptocurrency networks.

7.4. Spoofed IP DDoS Attacks Detection

The proposed solutions for DDoS attacks detection mainly identifies the source IP address and use blockchain technology to store the transactions and share the IP address among the stakeholders to block/whitelist the IP address with trust and validation at the network level [85][86] [87] [88] [85] [82] [89] [80]. These solutions assume that the originating malicious IP addresses are not spoofed, and this condition is not always true. In most of the scenarios, as seen in Table 2, the attacker performs a reflection attack, in which the spoofed traffic is being sent to the victim to consume the communication capacity or saturate the CPU or memory resources for successful DDoS attack. The researchers also have not addressed the IPv6 traffic and can be critical storing the IP version 6 data in blockchain in terms of memory consumption.

7.5. IoT and SDN Vendor Interoperability

The existing state-of-art essentially utilized the software-defined networks and internet of things technology to address the denial of service attacks either at the victim level or network level. Even though those solutions prove that the attacks can be mitigated, there is a real challenge when trying to adopt the techniques in the industry. The IoT device or gateway vendors are quite diversified, and there is a multitude of SDN supporting network device providers for an enterprise solution. We tend to see incompatibility issues and also supporting blockchain node issues in these network paradigms, and deploying a decentralized application across their stakeholder network is impractical. It is desirable to depend on Blockchain-based DDoS mitigation as a service solution like Gladius [109].

7.6. Blockchain based DDoS solution metrics

Our survey study reveals that most of the proposed blockchain based solutions address the DDoS attacks by designing new architectures, describing new algorithms or methods, or implementing the DDoS mitigation solutions using blockchain technologies such as Ethereum. None of those solutions determined the performance of the blockchain based DDoS attack solutions in terms of the metrics like Mean time to detect (MTD), the average number of transactions, or transaction appending time to the distributed ledger. The standard evaluation list of metrics may need to be proposed to determine the blockchain based DDoS attack mitigation solutions.

8. Conclusion

Blockchain has emerged as a disruptive technology in recent times and the blockchain application capabilities are promising to use in the field of cybersecurity. DDoS attacks are well known and still considered a major threat to disrupt businesses. We have performed a detailed review of the blockchain-based solutions for DDoS attacks detection and mitigation including the consideration of the different network environments such as SDN, IoT, cloud, or conventional networks. The solutions are categorized based on the solution deployment location such as network based, near attack location, near victim location, and hybrid solutions. We determined that most of the existing solutions focused on storing the malicious IP addresses in blockchain transactions implemented using smart contracts and distributing the IP addresses across the ASs at the network level. However, limited research is performed to propose near-victim location and hybrid solutions. Finally, we described the open challenges based on the existing research contributions and the future directions based on the advancements in blockchain technologies like parallel blockchain, Xroute, and Ethereum 2.0 to effectively handle DDoS attacks.

Our review can be a reference resource for readers and future researchers interested in pursuing research in the combination of Blockchain and DDoS attacks domain.

Funding

Not applicable.

Conflicts of interest/Competing interests

The authors declare no conflict of interest.

Availability of data and material

Code availability

References

[1] Real Security. Evolution of ddos in the last decade - real security. https://www.real-sec.com/2019/08/evolution-of-ddos-in-the-last-decade/. (Accessed on 06/10/2022).

[2] Nexusguard. Ddos threat report 2020 q2. https://blog.nexusguard.com/threat-report/ddos-threat-report-2020-q2, 2020. (Accessed on 06/10/2022).

[3] Lily Hay Newman. A 1.3-tbs ddos hit github, the largest yet recorded — wired. https://www.wired.com/story/github-ddos-memcached/, 2018. (Accessed on 06/03/2021).

[4] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

[5] Brian Krebs. Krebsonsecurity hit with record ddos – krebs on security. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, 2016. (Accessed on 06/25/2022).

[6] John Kennedy. Ovh suffers 1.5tbps ddos attack via 145,000 webcams. https://www.siliconrepublic.com/machines/mega-iot-cyberattack-ovh-suffers-1-5tbps-ddos-attack-via-145000-webcams, 2016. (Accessed on 06/15/2021).

[7] Shane Greenstein. The aftermath of the dyn ddos attack. *IEEE Micro*, 39(4):66–68, 2019.

[8] Xiaoying Zheng, Yongxin Zhu, and Xueming Si. A survey on challenges and progresses in blockchain technologies: A performance and security perspective. *Applied Sciences (Switzerland)*, 9(22):1–24, 2019.

[9] Zhetao Li, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8):3690–3700, 2018.

[10] Jiafu Wan, Jiapeng Li, Muhammad Imran, and Di Li. A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Transactions on Industrial Informatics*, 15(6):3652–3660, 2019.

[11] Junqin Huang, Linghe Kong, Guihai Chen, Min You Wu, Xue Liu, and Peng Zeng. Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. *IEEE Transactions on Industrial Informatics*, 15(6):3680–3689, 2019.

[12] Gaoqi Liang, Steven R. Weller, Fengji Luo, Junhua Zhao, and Zhao Yang Dong. Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks. *IEEE Transactions on Smart Grid*, 10(3):3162–3173, 2019.

[13] Ruinian Li, Tianyi Song, Bo Mei, Hong Li, Xiuzhen Cheng, and Limin Sun. Blockchain for Large-Scale Internet of Things Data Storage and Protection. *IEEE Transactions on Services Computing*, 12(5):762–771, 2019.

[14] Abbas Yazdinejad, Reza M. Parizi, Ali Dehghantanha, Qi Zhang, and Kim Kwang Raymond Choo. An Energy-Efficient SDN Controller Architecture for IoT Networks with Blockchain-Based Security. *IEEE Transactions on Services Computing*, 13(4):625–638, 2020.

[15] Zecheng Li, Shang Gao, Zhe Peng, Songtao Guo, Yuanyuan Yang, and Bin Xiao. B-DNS: A Secure and Efficient DNS Based on the Blockchain Technology. *IEEE Transactions on Network Science and Engineering*, 8(2):1674–1686, 2021.

[16] Yuan Zhang, Chunxiang Xu, Jianbing Ni, Hongwei Li, and Xuemin Sherman Shen. Blockchain-assisted Public-key Encryption with Keyword Search against Keyword Guessing Attacks for Cloud Storage. *IEEE Transactions on Cloud Computing*, PP(c):1, 2020.

[17] Bruno Rodrigues, Thomas Bocek, and Burkhard Stiller. Enabling a cooperative, multi-domain ddos defense by a blockchain signaling system (bloss). *Semantic Scholar*, 2017.

[18] Kyoungmin Kim, Youngin You, Mookyu Park, and Kyungho Lee. DDoS Mitigation: Decentralized CDN Using Private Blockchain. In *International Conference on Ubiquitous and Future Networks, ICUFN*, volume 2018-July, pages 693–696. IEEE Computer Society, 8 2018.

[19] Syed Badruddoja, Ram Dantu, Logan Widick, Zachary Zaccagni, and Kritagya Upadhyay. Integrating dots with blockchain can secure massive iot sensors. In *2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, pages 937–946. IEEE, 2020.

[20] Lo Yao Yeh, Peggy Joy Lu, Szu Hao Huang, and Jiun Long Huang. SOChain: A Privacy-Preserving DDoS Data Exchange Service Over SOC Consortium Blockchain. *IEEE Transactions on Engineering Management*, 2020.

[21] Noshina Tariq, Muhammad Asim, Feras Al-Obeidat, Muhammad Zubair Farooqi, Thar Baker, Mohammad Hammoudeh, and Ibrahim Ghafir. The security of big data in fog-enabled iot applications including blockchain: A survey. *Sensors (Switzerland)*, 19(8):1–33, 2019.

[22] Lucian Constantin. DDoS Attacks Against US Banks Peaked At 60 Gbps — CIO. https://www.cio.com/article/2389721/ddos-attacks-against-us-banks-peaked-at-60-gbps.html, 2012. (Accessed on 06/10/2021).

[23] Jaikumar Vijayan. Update: Spamhaus hit by biggest-ever DDoS attacks — Computerworld. https://www.computerworld.com/article/2495967/update–spamhaus-hit-by-biggest-ever-ddos-attacks.html, 2013.

[24] JON RUSSELL. Hong Kong Group Battles Huge DDoS Attack. https://tinyurl.com/2jfbb9vf, 2014.

[25] Cadie Thompson. Record-breaking DDoS attack strikes CloudFlareś network. https://www.cnbc.com/2014/02/11/record-breaking-ddos-attack-strikes-cloudflares-network.html, 2014.

[26] Damian Menscher. Identifying and protecting against the largest ddos attacks — google cloud blog. https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks, 2020. (Accessed on 06/25/2022).

[27] Amazon. AWS Shield Threat Landscape Report – Q1 2020. https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf, 2020. (Accessed on 06/05/2021).

[28] C. Douligeris and A. Mitrokotsa. DDoS attacks and defense mechanisms: A classification. *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2003*, pages 190–193, 2003.

[29] Vinayakumar Ravi, Rajasekhar Chaganti, and Mamoun Alazab. Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. *Computers and Electrical Engineering*, 102:108156, 2022.

[30] Rochak Swami, Mayank Dave, and Virender Ranga. Software-defined networking-based ddos defense mechanisms. *ACM Computing Surveys (CSUR)*, 52(2):1–36, 2019.

[31] Saif ur Rehman, Mubashir Khaliq, Syed Ibrahim Imtiaz, Aamir Rasool, Muhammad Shafiq, Abdul Rehman Javed, Zunera Jalil, and Ali Kashif Bashir. Diddos: An approach for detection and identification of distributed denial of service (ddos) cyberattacks using gated recurrent units (gru). *Future Generation Computer Systems*, 118:453–466, 2021.

[32] Marios Anagnostopoulos, Georgios Kambourakis, Panagiotis Kopanos, Georgios Louloudakis, and Stefanos Gritzalis. Dns amplification attack revisited. *Computers & Security*, 39:475–485, 2013.

[33] Sheng Hong, Juxing Zhu, Lidia A Braunstein, Tingdi Zhao, and Qiuju You. Cascading failure and recovery of spatially interdependent networks. *Journal of Statistical Mechanics: Theory and Experiment*, 2017(10):103208, 2017.

[34] Sheng Hong, Tianyu Yue, and Hao Liu. Vehicle energy system active defense: a health assessment of lithium-ion batteries. *International Journal of Intelligent Systems*, 2020.

[35] A Srivastava, BB Gupta, A Tyagi, Anupama Sharma, and Anupama Mishra. A recent survey on ddos attacks and defense mechanisms. In *International Conference on Parallel Distributed Computing Technologies and Applications*, pages 570–580. Springer, 2011.

[36] Catalin Cimpanu. Ddos botnets have abused three zero-days in lilin video recorders for months — zdnet. https://www.zdnet.com/article/ddos-botnets-have-abused-three-zero-days-in-lilin-video-recorders-for-months/, 2020. (Accessed on 06/10/2021).

[37] Saman Taghavi Zargar, James Joshi, and David Tipper. A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. *IEEE Communications Surveys and Tutorials*, 15(4):2046–2069, 2013.

[38] Sheng Hong, Chuan Lv, Tingdi Zhao, Baoqing Wang, Jianghui Wang, and Juxing Zhu. Cascading failure analysis and restoration strategy in an interdependent network. *Journal of Physics A: Mathematical and Theoretical*, 49(19):195101, 2016.

[39] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[40] Cryptocurrency Prices, Charts And Market Capitalizations — CoinMarketCap. https://coinmarketcap.com/, 2021.

[41] Anthony Albertorio. Public Key Cryptography and Digital Signatures. https://tinyurl.com/3cebahnn, 2018.

[42] Julija Golosova and Andrejs Romanovs. The advantages and disadvantages of the blockchain technology. In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*, pages 1–6. IEEE, 2018.

[43] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. Ieee, 2017.

[44] Nathan Reiff. 10 important cryptocurrencies other than bitcoin. https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/, 2020. (Accessed on 06/21/2021).

[45] Rene Millman. What is Ethereum 2.0 and Why Does It Matter? - Decrypt. https://decrypt.co/resources/what-is-ethereum-2-0, 2020. (Accessed on 06/15/2021.

[46] Github hyperledger/fabric:. https://github.com/hyperledger/fabric, 2022. (Accessed on 06/10/2021).

[47] Girad. The iot rundown for 2020: Stats, risks, and solutions – security today. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2, 2020. (Accessed on 06/25/2022).

[48] Balkis Bettoumi and Ridha Bouallegue. Lc-dex: Lightweight and efficient compressed authentication based elliptic curve cryptography in multi-hop 6lowpan wireless sensor networks in hip-based internet of things. *Sensors*, 21(21):7348, 2021.

[49] Chafika Benzaid, Karim Lounis, Ameer Al-Nemrat, Nadjib Badache, and Mamoun Alazab. Fast authentication in wireless sensor networks. *Future Generation Computer Systems*, 55:362–375, 2016.

[50] Hamed HaddadPajouh, Ali Dehghantanha, Reza M Parizi, Mohammed Aledhari, and Hadis Karimipour. A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, 14:100129, 2021.

[51] Kannan Govindarajan, Kong Chee Meng, and Hong Ong. A literature review on software-defined networking (sdn) research topics, challenges and solutions. In *2013 fifth International conference on advanced computing (ICoAC)*, pages 293–299. IEEE, 2013.

[52] Rajendra V Boppana, Rajasekhar Chaganti, and Vasudha Vedula. Analyzing the vulnerabilities introduced by ddos mitigation techniques for software-defined networks. In *National Cyber Summit*, pages 169–184. Springer, 2019.

[53] Liuwei Huo, Dingde Jiang, Sheng Qi, and Lei Miao. A Blockchain-Based Security Traffic Measurement Approach to Software Defined Networking. *Mobile Networks and Applications*, pages 1–11, 1 2020.

[54] Pat Bosshart, Dan Daly, Glen Gibb, Martin Izzard, Nick Mckeown, Jennifer Rexford, Cole Schlesinger, Dan Talayco, Amin Vahdat, George Varghese, and David Walker. P4: Programming Protocol-Independent Packet Processors. Technical report.

[55] Mousa Taghizadeh Manavi. Defense mechanisms against distributed denial of service attacks: A survey. *Computers & Electrical Engineering*, 72:26–38, 2018.

[56] Ruchi Vishwakarma and Ankit Kumar Jain. A survey of ddos attacking techniques and defence mechanisms in the iot network. *Telecommunication systems*, 73(1):3–25, 2020.

[57] Rami J Alzahrani and Ahmed Alzahrani. Security analysis of ddos attacks using machine learning algorithms in networks traffic. *Electronics*, 10(23):2919, 2021.

[58] Narmeen Zakaria Bawany, Jawwad A Shamsi, and Khaled Salah. Ddos attack detection and mitigation using sdn: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, 42(2):425–441, 2017.

[59] Zawar Shah, Imdad Ullah, Huiling Li, Andrew Levula, and Khawar Khurshid. Blockchain based solutions to mitigate distributed denial of service (ddos) attacks in the internet of things (iot): A survey. *Sensors*, 22(3):1094, 2022.

[60] Sharyar Wani, Mohammed Imthiyas, Hamad Almohamedh, Khalid M Alhamed, Sultan Almotairi, and Yonis Gulzar. Distributed denial of service (ddos) mitigation using blockchain—a comprehensive insight. *Symmetry*, 13(2):227, 2021.

[61] Rajeev Singh, Sudeep Tanwar, and Teek Parval Sharma. Utilization of blockchain for mitigating the distributed denial of service attacks. *Security and Privacy*, 3(3), 5 2020.

[62] Iuon-Chang Lin and Tzu-Chun Liao. A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 19(5):653–659, 2017.

[63] Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, and Syed Hassan Ahmed. A review of current security issues in internet of things. In *EAI/Springer Innovations in Communication and Computing*, pages 11–23. Springer Science and Business Media Deutschland GmbH, 2019.

[64] Ammar Muthanna, Abdelhamied A. Ateya, Abdukodir Khakimov, Irina Gudkova, Abdelrahman Abuarqoub, Konstantin Samouylov, and Andrey Koucheryavy. Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. *Journal of Sensor and Actuator Networks*, 8(1), 2019.

[65] Xianmin Wang, Jing Li, Xiaohui Kuang, Yu an Tan, and Jin Li. The security of machine learning in an adversarial setting: A survey. *Journal of Parallel and Distributed Computing*, 130:12–23, 8 2019.

[66] Shang Gao, Zecheng Li, Bin Xiao, and Guiyi Wei. Security Threats in the Data Plane of Software-Defined Networks. *IEEE Network*, 32(4):108–113, 7 2018.

[67] Chao Qu, Ming Tao, and Ruifen Yuan. A hypergraph-based blockchain model and application in internet of things-enabled smart homes. *Sensors (Switzerland)*, 18(9), 2018.

[68] Felipe S. Dantas Silva, Esau Silva, Emidio P. Neto, Marcilio Lemos, Augusto J. Venancio Neto, and Flavio Esposito. A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. *Sensors (Switzerland)*, 20(11):1–28, 2020.

[69] Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar, and Rajani Singh. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors (Switzerland)*, 19(2):1–17, 2019.

[70] Shailendra Rathore, Yi Pan, and Jong Hyuk Park. BlockDeepNet: A blockchain-based secure deep learning for IoT network. *Sustainability (Switzerland)*, 11(14):1–15, 2019.

[71] Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys and Tutorials*, 22(3):1686–1721, 7 2020.

[72] Kelton A.P. da Costa, João P. Papa, Celso O. Lisboa, Roberto Munoz, and Victor Hugo C. de Albuquerque.

Internet of Things: A survey on machine learning-based intrusion detection approaches. *Computer Networks*, 151:147–157, 3 2019.

[73] Shi Dong, Khushnood Abbas, and Raj Jain. A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. *IEEE Access*, 7:80813–80828, 2019.

[74] Kaijun Liu, Shengwei Xu, Guoai Xu, Miao Zhang, Dawei Sun, and Haifeng Liu. A Review of Android Malware Detection Approaches Based on Machine Learning. *IEEE Access*, 8:124579–124607, 2020.

[75] Vasiliy Elagin, Anastasia Spirkina, Andrei Levakov, and Ilya Belozertsev. Blockchain behavioral traffic model as a tool to influence service IT security. *Future Internet*, 12(4):1–12, 2020.

[76] P. J. Beslin Pajila and E. Golden Julie. Detection of DDoS Attack Using SDN in IoT: A Survey. In *Lecture Notes on Data Engineering and Communications Technologies*, volume 33, pages 438–452. Springer, 2 2020.

[77] Krushang Sonar and Hardik Upadhyay. A survey: Ddos attack on internet of things. *International Journal of Engineering Research and Development*, 10(11):58–63, 2014.

[78] Jin Ho Park and Jong Hyuk Park. Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, 9(8):1–13, 2017.

[79] Bruno Rodrigues, Thomas Bocek, Andri Lareida, David Hausheer, Sina Rafati, and Burkhard Stiller. A blockchain-based architecture for collaborative ddos mitigation with smart contracts. In *IFIP International Conference on Autonomous Infrastructure, Management and Security*, pages 16–29. Springer, Cham, 2017.

[80] Jonathan Burger. Jonathan burger-ba.pdf. https://files.ifi.uzh.ch/CSG/staff/Rafati/Jonathan%20Burger-BA.pdf, 2017. (Accessed on 06/25/2022).

[81] Uzair Javaid, Ang Kiang Siang, Muhammad Naveed Aman, and Biplab Sikdar. Mitigating lot device based ddos attacks using blockchain. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pages 71–76, 2018.

[82] Kotaro Kataoka, Saurabh Gangwar, and Prashanth Podili. Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN. In *IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings*, volume 2018-Janua, pages 296–301. Institute of Electrical and Electronics Engineers Inc., 5 2018.

[83] Mohammad Tayyab, Bahari Belaton, and Mohammed Anbar. ICMPv6-Based DoS and DDoS Attacks Detection Using Machine Learning Techniques, Open Challenges, and Blockchain Applicability: A Review. *IEEE Access*, 8:170529–170547, 9 2020.

[84] Adam Pavlidis, Marinos Dimolianis, Kostas Giotis, Loukas Anagnostou, Nikolaos Kostopoulos, Theocharis Tsigkritis, Ilias Kotinas, Dimitrios Kalogeras, and Vasilis Maglaris. Orchestrating DDoS mitigation via blockchain-based network provider collaborations. *Knowledge Engineering Review*, 35, 2020.

[85] Zakaria Abou, El Houda, Abdelhakim Hafid, and Lyes Khoukhi. Co-IoT: A Collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN. *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2019.

[86] Lo-Yao Yeh, Jiun-Long Huang, Ting-Yin Yen, and Jen-Wei Hu. A collaborative ddos defense platform based on blockchain technology. In *2019 Twelfth International Conference on Ubi-Media Computing (Ubi-Media)*, pages 1–6. IEEE, 2019.

[87] Meryam Essaid, DaeYong Kim, Soo Hoon Maeng, Sejin Park, and Hong Taek Ju. A collaborative ddos mitigation solution based on ethereum smart contract and rnn-lstm. In *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pages 1–6. IEEE, 2019.

[88] Xue Yang, Bingyang Liu, Fei Yang, and Chuang Wang. A blockchain based online trading system for ddos mitigation services. In *2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, pages 1036–1037. IEEE, 2018.

[89] Bruno Rodrigues, Thomas Bocek, and Burkhard Stiller. Multi-domain ddos mitigation based on blockchains. In *IFIP International Conference on Autonomous Infrastructure, Management and Security*, pages 185–190. Springer, 2017.

[90] Moses Sam Paul. Deploy Smart Contracts on Ropsten Testnet through Ethereum Remix. https://tinyurl.com/nymnyc5c, 2018. (Accessed on 06/15/2021).

[91] Mehrdad Hajizadeh, Nima Afraz, Marco Ruffini, and Thomas Bauschert. Collaborative cyber attack defense in sdn networks using blockchain technology. In *2020*

6th IEEE Conference on Network Softwarization (NetSoft), pages 487–492. IEEE, 2020.

[92] Gagangeet Singh Aujla, Maninderpal Singh, Arnab Bose, Neeraj Kumar, Guangjie Han, and Rajkumar Buyya. BlockSDN: Blockchain as a Service for Software Defined Networking in Smart City Applications. *IEEE Network*, 34(2):83–91, 3 2020.

[93] Qaisar Shafi and Abdul Basit. Ddos botnet prevention using blockchain in software defined internet of things. In *2019 16th international Bhurban conference on applied sciences and technology (IBCAST)*, pages 624–628. IEEE, 2019.

[94] Zakaria Abou El Houda, Abdelhakim Senhaji Hafid, and Lyes Khoukhi. Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract. *IEEE Access*, 7:98893–98907, 2019.

[95] DVVS Manikumar and B Uma Maheswari. Blockchain based ddos mitigation using machine learning techniques. In *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pages 794–800. IEEE, 2020.

[96] Meizhu Chen, Xiangyan Tang, Jieren Cheng, Naixue Xiong, Jun Li, and Dong Fan. A ddos attack defense method based on blockchain for iots devices. In *International Conference on Artificial Intelligence and Security*, pages 685–694. Springer, 2020.

[97] Gokhan Sagirlar, Barbara Carminati, and Elena Ferrari. AutoBotCatcher: Blockchain-based P2P botnet detection for the internet of things. In *Proceedings - 4th IEEE International Conference on Collaboration and Internet Computing, CIC 2018*, pages 1–8. Institute of Electrical and Electronics Engineers Inc., 11 2018.

[98] Georgios Spathoulas, Nikolaos Giachoudis, Georgios Paraskevas Damiris, and Georgios Theodoridis. Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets. *Future Internet*, 11(11), 11 2019.

[99] Syed Muhammad Sajjad, Muhammad Rafiq Mufti, Muhammad Yousaf, Waqar Aslam, Reem Alshahrani, Nadhem Nemri, Humaira Afzal, Muhammad Asghar Khan, and Chien-Ming Chen. Detection and blockchain-based collaborative mitigation of internet of things botnets. *Wireless Communications and Mobile Computing*, 2022, 2022.

[100] Shanqing Jiang, Lin Yang, Xianming Gao, Yuyang Zhou, Tao Feng, Yanbo Song, Kexian Liu, and Guang Cheng. Bsd-guard: A collaborative blockchain-based approach for detection and mitigation of sdn-targeted ddos attacks. *Security and Communication Networks*, 2022, 2022.

[101] Rana Faisal Hayat, Sana Aurangzeb, Muhammad Aleem, Gautam Srivastava, and Jerry Chun-Wei Lin. Ml-ddos: A blockchain-based multilevel ddos mitigation mechanism for iot environments. *IEEE Transactions on Engineering Management*, 2022.

[102] Paralism commercial white paper – paralism blog. https://www.paralism.com/blog/paralism-commercial-white-paper/, 2019. (Accessed on 06/05/2021).

[103] Introducing XRouter: Developers Can Now Mix And Match Any Blockchain Via The World's First Blockchain Router. https://tinyurl.com/m89h9cnv, 2019. (Accessed on 06/05/2021.

[104] Sarwar Sayeed and Hector Marco-Gisbert. Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied sciences*, 9(9):1788, 2019.

[105] Guangquan Xu, Bingjiang Guo, Chunhua Su, Xi Zheng, Kaitai Liang, Duncan S Wong, and Hao Wang. Am i eclipsed? a smart detector of eclipse attacks for ethereum. *Computers & Security*, 88:101604, 2020.

[106] Muhammad Saad, Laurent Njilla, Charles Kamhoua, Joongheon Kim, DaeHun Nyang, and Aziz Mohaisen. Mempool optimization for defending against ddos attacks in pow-based blockchain systems. In *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)*, pages 285–292. IEEE, 2019.

[107] How Ethereum lost $300 Million Dollars — Hacker Noon. https://hackernoon.com/how-ethereum-lost-300-million-dollars-bfedf7ba0c19, 2017. (Accessed on 06/15/2021.

[108] Tyler Vasek, Marie; Thornton, Micah; Moore. Replication data for: Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. https://dataverse.harvard.edu/dataset.xhtml?persistentIddoi:10.7910D (Accessed on 06/03/2021).

[109] Gladius: CDN Decentralized And DDoS Protection On The Blockchain. https://tinyurl.com/hmjd5s9u, 2017. (Accessed on 06/15/2021).