IoT

MDPI

Article

Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things

Diego Mendez Mena and Baijian Yang *

Department of Computer and Information Technology, Purdue University, West Lafayette, IN 47907, USA; dmendezm@purdue.edu

* Correspondence: byang@purdue.edu

Abstract: Security presents itself as one of the biggest threats to the enabling and the deployment of the Internet of Things (IoT). Security challenges are evident in light of recent cybersecurity attacks that targeted major internet service providers and crippled a significant portion of the entire Internet by taking advantage of faulty and ill-protected embedded devices. Many of these devices reside at home networks with user-administrators who are not familiar with network security best practices, making them easy targets for the attackers. Therefore, security solutions are needed to navigate the insecure and untrusted public networks by automating protections through affordable and accessible first-hand network information sharing. This paper proposes and implements a proof of concept (PoC) to secure Internet Service Providers (ISPs), home networks, and home-based IoT devices using blockchain technologies. The results obtained support the idea of a distributed cyber threat intelligence data sharing network capable of protecting various stakeholders.

Keywords: network security; blockchain; Internet of Things; cyber threat intelligence

Citation: Mendez Mena, D.; Yang, B. Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things. *IoT* **2021**, *2*, 1–16. https://doi.org/10.3390/iot2010001

Received: 17 November 2020
Accepted: 26 December 2020
Published: 30 December 2020

1. Introduction

The Internet of Things (IoT) is constituted of resource-limited devices connected to the Internet and interacting with other entities in the network, with or without direct human intervention. The main objective of IoT is to provide ubiquitous connectivity among different entities or "things" [1]. While the performance, effectiveness, and efficiency of IoT have improved significantly over a short period of time, the security aspect of the IoT and the network it sits remain a very challenging issue. In 2016, a Distributed Denial of Service (DDoS) attack was enabled by a botnet army of IoT infected devices. It not only overwhelmed Dyn, a major domain name system (DNS) infrastructure provider, but also paralyzed a significant portion of the Internet. The incident highlighted the alarming consequence that faulty IoT protections and poor security standards could incur [2]. Such intrusions and attacks accentuate the need for additional research in the IoT security domain.

The search for energy efficiency and affordable computing power on embedded devices is in some way antagonistic to current cryptography applications and security solutions, which describes a paradox that produces a challenging environment for the IoT [1]. The newly hyped blockchain technology proposes new ways to securely exchange digital assets by the use of strong cryptography principles and sound engineering protocols. Although it was meant to be the building block of cryptocurrency, blockchain has found its way through other realms. This includes the possibility to address security challenges, an area that is far from its original conception [3].

The purpose of this work is to introduce an application of the blockchain protocol to protect end-to-end network functionality, from the service providers to the edge of the home network, and hence the IoT devices in it. The work greatly extended the primary idea of our earlier work [4]. In addition, this work proposes a security framework that supports deeper interactions between service providers and their consumers. And finally,

it lays out the possibility to create a democratic cyber threat intelligence (CTI) network capable of enforcing proactive and reactive countermeasures to cyberattacks.

The rest of the paper is organized as follows. Related works are reviewed in Section 2, followed by the research design and method in Section 3. Section 4 illustrates the results, and more in-depth discussions of the work can be found in Section 5. Finally, Section 6 summarizes the findings of the study and sheds light on future work.

2. Literature Review

During the last few years, the total number of IoT devices and the data they processed have increased significantly [1]. IoT devices have found their way to support more applications and reached more home users. The ubiquitousness of IoT brings both advantages and challenges to the end-users. The authors of Reference [5] identified the following as the most common vulnerabilities: Insecure web interfaces, insufficient authentication, insecure network services, poor privacy controls, insufficient security configurability, insecure software, and poor physical security. Since IoT devices are constantly online, the weak security protections, or no protection at all, made them easy targets of infections and becoming zombies of botnets [6]. Cui and Stolfo [7] scanned IoT devices on the Internet for basic security probes. They discovered over 540,000 exposed devices, with many using the default login credentials created by the vendors. The authors of Reference [8] analyzed the firmware of 32,000 IoT devices. Over 2000 devices had backdoor access, such as telnet service with hard-coded passwords. From the perspectives of regular users, the difficulty of managing home networks, the lack of security policy mandate, and the ever-rising security risks and attacks place an overwhelming burden on the shoulders of end consumers [9].

Mahmoud et al. [10] provided a more organized view of IoT challenges by classifying them regarding its architecture. At the perception layer, wireless communications interference, interception, or alteration (replay attacks), and physical security must be considered. The network layer is susceptible to DoS and eavesdropping attacks, mostly due to the weak authentication of IoT devices. At the application layer, security problems were the result of the heterogeneous nature of IoT. The lack of governing policies and standards further complicated the situation and some products may have adopted conflicting authentication mechanisms. Reference [11] stated that weak passwords, dissimilar storage and data processing methods, flawed security controls, and insufficient filtering capacity are the main reasons for IoT devices to miscarry privacy, trust, confidentiality, identity attestation, and access enforcement. Reference [12] accounted faulty identification integrity, lack of global authentication schemes, poor privacy strategies (data collection policies and data anonymization), insufficient lightweight cryptographic solutions, deficient software development practices and software analysis constraints, as well as malicious software for the IoT security panorama. Pacheco et al. [13] added Internet network extension (from mobile, non-IP, sensor to cloud and fog computing), multiple entry points, and domain diversity (on ownership, policy, and connectivity) to the list of obstacles. Reference [14] stressed that inadequate perimeter defenses, host-based detection mechanisms, and patching processes designed for the IoT environment are the key dimensions that need to be addressed. Finally, Reference [15] broke IoT security issues into two main topics: Data security and privacy protection. In summary, the security breadth has expanded exponentially but the available resources are not sufficient to cope with the ongoing environment. The challenges identified are not trivial to define and even harder to solve. From this literature review, it is evident that IoT security consensus needs to be reached and prioritization needs to be listed before the research community advocating for action.

The Mirai botnet attack in 2016 was a consequence of the lack of security implementations of embedded devices. The attack was considered "one of the most potent Distributed-Denial-of-Service (DDoS) attacks in history" [6]. Over 400,000 devices were compromised that included webcams, DVRs, home routers, etc. Altogether, the botnet delivered over 1.1 Tbps of traffic to bring down French provider OVH. Mirai used hard-coded default credentials to brute force access that were available over port 23 and 223.

Once compromised, the command and control (C&C) center launched General Routing Encapsulation (GRE), Transfer Control Protocol (TCP), and Hypertext Transfer Protocol (HTTP) flooding attacks on the targets to take them out of service. Similar attacks are still being deployed over the Internet despite the warnings from the security community for keeping susceptible devices openly accessible [6].

The blockchain, based on its security properties, has attracted more attention from the IoT research community. IoT researchers cataloged the blockchain as one of the key technologies capable of enabling smart contracts among embedded devices [16]. This means smart embedded devices can autonomously interact with each other without human intervention. Smart contracts enable IoT devices to build functionality based on their previous states and desired outputs.

Even though it is feasible to implement a public blockchain network, the computing power required for mining may be overwhelming, especially when billions of IoT devices need to be addressed. Therefore, for many applications, private or consortium blockchain solve some of the initial trust concerns among members, where alternative consensus algorithms and other access techniques can be leveraged to reduce the burden of mining and make blockchains much more desirable in real-world practice. It should be noted that blockchains offer only pseudo-anonymity: it is possible for adversaries to make inferences about who owns what public keys. If privacy is a major concern in an IoT system, an additional mechanism must be designed and implemented to prevent the owners of the smart devices from being identified. For instance, the authors of Reference [17] have identified several applications that can be benefited from blockchain solutions, including identity management and authentication requirements for securing network infrastructure without a central authority. Azaria et al. [18] and Zyskind et al. [19] further applied the blockchain and smart contracts to secure sensitive data, which allows users to access it without being tampered.

Cyber Threat Intelligence (CTI) is evidence-based information that is valuable, relevant, and actionable for security professionals. It can shorten the time between compromises and detection and therefore proactively answer the security challenges that need attention [20]. S. Jasper [21] mentioned sensitive information, classification, trust, interoperability, and privacy as the main reasons entities are reluctant to share CTI data. Tounsi and Rais [20] also claimed that quality issues, budgeting, and the lack of legal confidence are the main problems CTI sharing brings to the table. Wagner et al. Reference [22] stressed the importance of having reliable sources. The information gathered and utilized must be conducted in a coordinated manner to ensure successful incident responses. To better leverage IoT CTI, it is best that the secure methods do not assume central trust while offering equal access and quick propagation and action. A blockchain network is a great candidate for such secure methods, as shown by Cha et al. [23]. They proposed a blockchain-based CTI system architecture for sustainable computing and used a blockchain network to provide sensitive data sharing.

Consequently, the authors would like to provide a quick review of their previous work [4]. The authors presented a blockchain-based security solution for home networks and home IoT devices. The authors relied on hardware implementations with known IoT "Smart Home" devices and created a practical testing environment. Statistical analyses were conducted to examine the numerical data obtained from the experiments and comparisons were made to understand the performance penalties the blockchain incurred against simple centralized security solutions.

A private Proof-of-Work Ethereum network was configured on three different machines. One of them operated at the perimeter of the home network, called "gatekeeper". The computer involved was assigned private Ethereum accounts that linked the users, the gatekeeper, and other components of the Ethereum blockchain and served as the interface of the system. The gatekeeper keeps a whitelist based on layer three information. The whitelist can be modified and updated by a smart contract that governs the system. The smart contract provides access to the home network.

The users interact with the contract through a solidity-based application, where layer three network information is entered and a hash value is used for integrity. The gatekeeper, using a Python script, reads blockchain transactions and adds entries to the whitelist based on information in the data field of the block. Figure 1 shows how the application was structured.

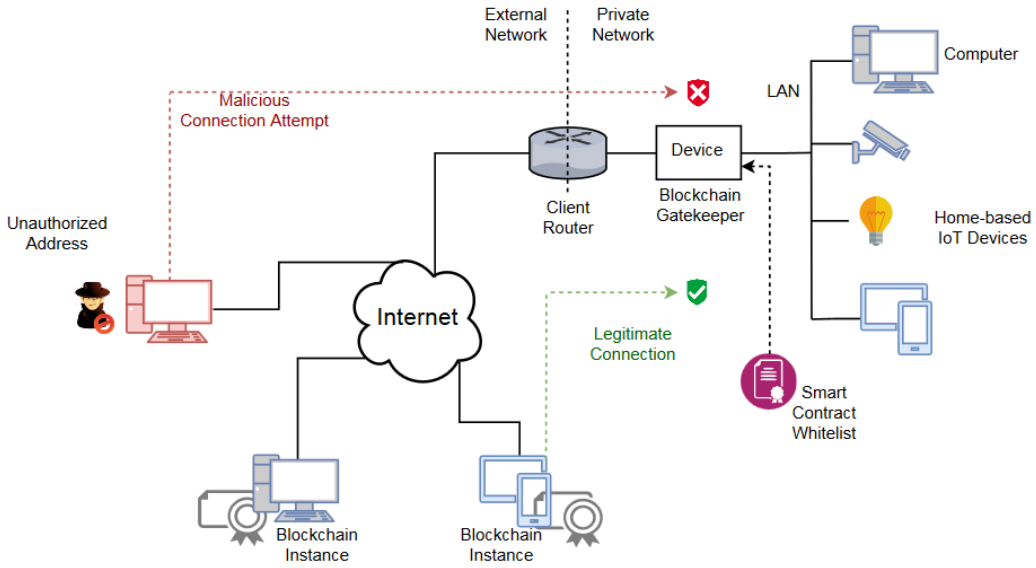

Figure 1. Network and logical diagram from previous work, taken from Reference [4].

The authors collected resource data at the gatekeeper and a client computer (miner) from two instances of the same implementation. The first instance ran a basic whitelisting on IPTables hosted by a Raspberry Pi (Gatekeeper) device. In other words, the baseline has no blockchain interaction. The second instance runs all blockchain operations described above. The data collected were statistically analyzed to compare both scenarios.

At the client computer, the CPU utilization and RAM usage presented statistically significant differences that showed a numerical increase during blockchain functioning. However, the disk usage did not show significant differences, even though over 70,000 blocks were processed during the sampling time frame. At the Gatekeeper, the CPU utilization and RAM usage showed significant differences. Nevertheless, the overall CPU usage did not go over 2%, and the RAM usage did not surpass 51%, which means no resource scarcity was experienced. As occurred with the client computer, no disk utilization differences were spotted.

The authors concluded that basic whitelisting applications based on blockchain technology to secure home-based networks and IoT devices were possible. Moreover, the inherent security properties of blockchain provided additional protection against malicious tampering of whitelist entries. The cryptographic features of the Ethereum protocol, such as asymmetric key encryption and digital signatures, strengthened peer-to-peer communications between the network nodes. The authors considered that the results could be qualified as the starting point to a secure home-based network architecture model for IoT devices. Additionally, the distributed computing properties of the blockchain open the door to future opportunities for decentralized cyber intelligence information secure sharing.

3. Materials and Methods

Malicious traffic is considered a burden for users and service providers (SP) [24]. Therefore, there exists the need to decrease the existing risks at home networks and ISPs' networks by stopping verified malicious indicators of compromise (IOC). The proposed solution aims to offer close to real-time containment for, but not limited to, network-based IOC. It collects first-hand information from the end-users and distributively shares the cyber threat intelligence (CTI) information via a consortium blockchain network.

During recent years, researchers have started to discuss further blockchain capabilities and applications. Atlam et al. [25] listed the blockchain characteristics that are appealing for addressing IoT challenges, including information immutability, decentralization, anonymity (after applying public key principles to the protocol), resiliency, trust, and increased computing capacity (by distributing computing). Ølnes et al. [26] showed benefits and promises of the blockchain presented in the academic literature that adds transparency, auditability, increased control (by consensus), data integrity, error reduction (by automation), enhanced access to information, reliability, data security (due to decentralization), and decreasing transaction costs (by no human involvement). Hughes et al. [27] indicated that settlement and reconciliation processes between different organizations could benefit from the simplicity and efficiency provided by the blockchain that translates to "significant cost savings" (p. 119) by automation, streamlined processes (by smart contract enforcing), and increased processing speed (due to disintermediation). However, the same authors [25–27] also emphasized the limitations of the blockchain technology, which includes processing power, storage capabilities over time, scalability, computing costs, and privacy concerns. The applicability of potential benefits also depends on design decisions and application buildout process [26], which suggests that not all the security gaps can be bridged by blockchain technology.

As cyber-threats constantly emerge, the focus of this work to explore the challenges and requirements that Cyber Threat Intelligence (CTI) information sharing is currently facing. New attack vectors make it burdensome for individual defenders to protect their digital assets by themselves. The only viable pathway is to build solutions by sharing reliable and trustworthy information with the community, an approach that has been taken by many organizations [28]. Böhm et al. [29] specified that such exchange of information can significantly improve cyber-defense capabilities, information that needs to be "integrity-proof" (p. 2). Mtsweni and Mutemwa [30] advocated for relevant and reliable data (with the appropriate volume) that is generated and shared with velocity and veracity. Even though the benefits of sharing intelligence information seem to be overwhelming, there exist security, privacy, and competitiveness concerns that prevent organizations to share valuable first-hand data at the expense of the community and the quality of the data [28]. Then, it is also important to sustain data quality without "free-riding" by auditing fair and equal participation from all actors while keeping privacy and anonymity. It is also important to consider the entire organization spectrum. Each unit, from small businesses to multi-nationals and from single users to structured corporations, is capable of providing and receiving valuable information. But each unit may have a different budget and priorities when it comes CIT. For instance, in developing countries and some smaller organizations, the main focus is to increase profits by cutting down expenses. The owners would probably like to take the risk by not participating CTI due to the lack of funding [31,32]. There are also quality differences in the CTI reports. Commercial sources often include structured data while open communities often share information without structure, "such as PDF and Word documents" [33] (p. 375). It is reasonable, then, to also advocate for the democratization of the threat intelligence data access.

The blockchain can provide highly-available data sharing between users and their Internet Service Providers (ISPs), as well as between different ISPs. A transparent and distributed CTI tamper-proof repository, capable of democratizing the access to the data [34], can be built and acted locally, at the user level, or at the ISP level. A decentralized and tamper-proof solution is now introduced with proof-of-concept capabilities for delivering vetted transparent CTI information. Corresponding actions can be enforced either at the source or at the destination of malicious activities. Literature shows different approaches to the existing gaps in CTI sharing. Blockchain technologies were proposed as a sustainable computing architecture to share computing power for efficiency [23]. Blockchains were also leveraged to address the trust and quality issue to engage participation in CTI contribution [35]. Büber et al. [36] proposed a voting/consensus system to add entries into a CTI database. Hajizadeh et al. [37] used the blockchain to control software-defined networking (SND)

systems to mitigate threats based on intelligence collaboration. In addition, Purohit et al. [38] proposed the utilization of the blockchain to share intelligence to fight against threats that are targeted at cloud-based services, such as free-riding and false reporting, by defining quality metrics. The work presented in this paper proposes the utilization of first-hand data from the end-users, their network components, such as IoT devices or service providers, and their detection systems to share intelligence information using the blockchain. The goal of this decentralized design is to be able to address various issues in the current CIT platforms, including trust, integrity, reliability, resiliency, and unequal information access.

3.1. Materials

In order to provide a proof-of-concept of the current solution proposal, the authors have designed a simulation environment that represents network actors and behavior of real conditions. Microsoft Azure was chosen as the simulation platform based on its nested virtualization properties and available resources for similar implementations. The virtual network is composed, first, of an Ubuntu server that serves as the administration gateway to the rest of the network connected directly to the internet. In the second place, the GNS3 server, a Linux-based virtual machine connected through TCP port 3080 with the local client, where all GNS3 computations are performed. And last, a series of Ubuntu-based clones running the same software load are used to implement the Ethereum blockchain network. The above design provides flexibility and scalability to the simulation structure as computer resources can be dynamically reallocated and the network nodes can be easily multiplied with minimum efforts. Figure 2 describes the location and the connection of the components of in the simulation.

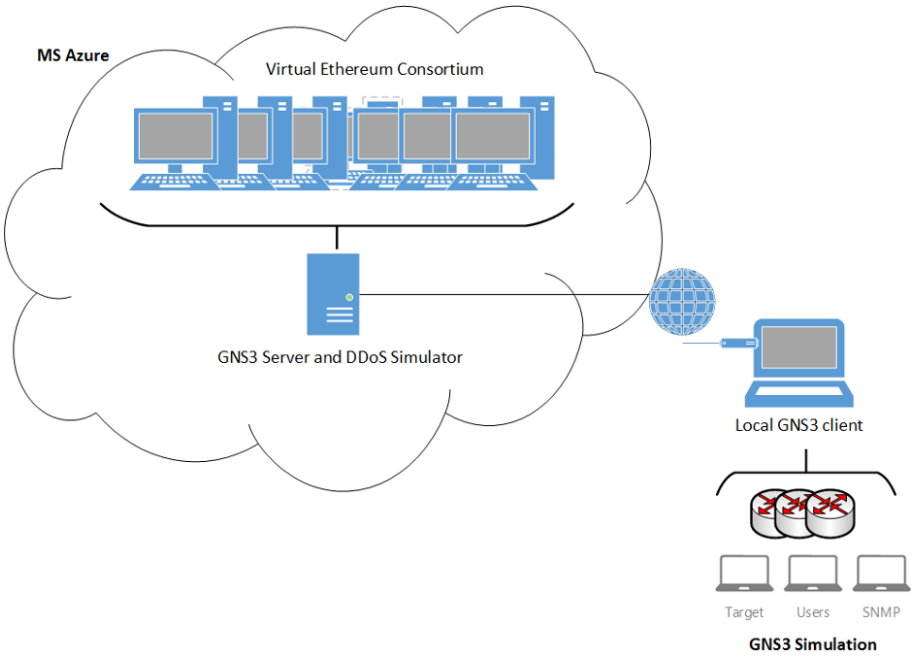

Figure 2. Connectivity scheme of the network simulation environment.

Figure 3 shows the implementation of the blockchain network proposed for the simulation. The backbone of the Ethereum network, and its resources, are simulated over the Microsoft Azure Ethereum proof-of-authority consortium template. Utilizing the Azure platform provides scalability and performance upgrades that do not interfere with the IP network simulation and its resources. The Microsoft Azure Ethereum template provides the capability to implement transaction and validator nodes under a consortium blockchain scheme that resembles the original network structure of this framework proposal. The consortium is composed of a leader and secondary members that reach administration and transaction consensus over the original blockchain principles. The underlying resources

for the consortium leader and its members are the same. However, the leader oversees the starting network configurations. It retains administrator privileges until it decides to distribute it among its peers.

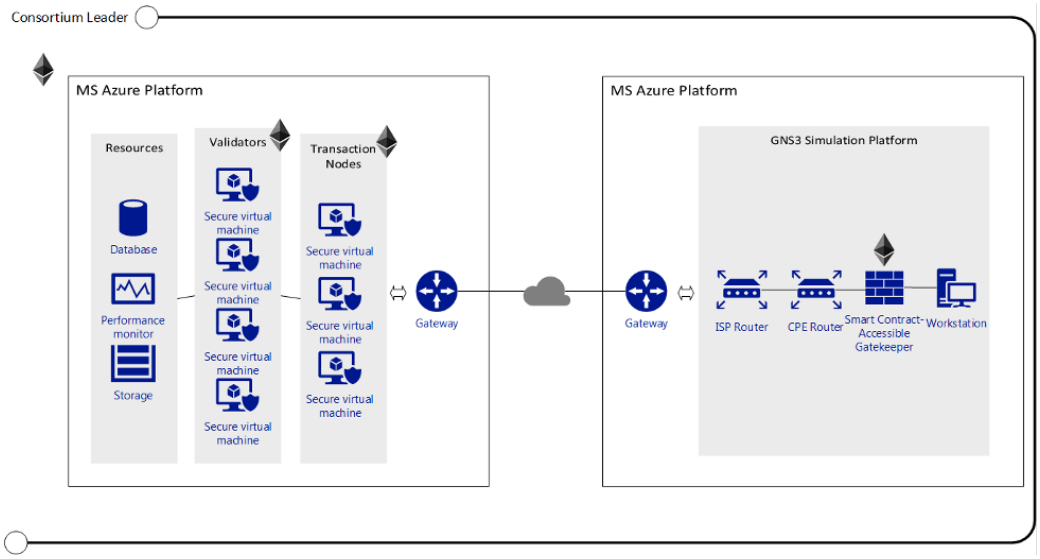

Figure 3. Ethereum consortium leader network scheme.

A unique permissioned blockchain network is needed, governed by two different types of smart contracts that would separate the network into two tiers. The first tier is composed of only the system end-users and their respective service provider. This is to maintain privacy and remove direct threats from the external actors. The second tier is constituted of all participating service providers that are used to exchange CTI information without including the direct participation from the end-users. The network blockchain validators employ the Proof-of-Authority consensus algorithm as it provides efficiency in terms of computing power over resource-intensive Proof-of-Work deployments.

3.2. Methods

A Distributed Denial of Service (DDoS) attack is simulated using the open-source tool Bonesi. The simulation tool is capable of generating ICMP, UDP, and TCP traffic replicating random IP addresses (spoofing). Under the current network configuration, up to 40,000 simulated bots can recreate over 150,000 packets per second, targeting a predetermined host located within "user" network boundaries. The tool can be used to recreate botnet behaviors, such as Mirai, by performing GRE IP and GRE ETH floods, SYN and ACK floods, STOMP floods, DNS floods, and UDP flood attacks [39]. The purpose of the simulation is to demonstrate that the proposed security framework can stop local bot traffic (after infection) and mitigate ISP network resource consumption, and target resource alleviation under a DDos attack. The simulation can also provide evidence of the framework's effectiveness under other types of cyberattacks from different infection stages, such as port and vulnerability scanning, and malware network propagation.

The framework simulation can be analyzed from three different categories: network performance, Ethereum network performance, and network security capabilities. In order to understand the impact of the implementation of a blockchain application sustained among the existing ISP resources, the experiment monitors memory, CPU, and link usage of the different network equipment that interacts with the framework. In addition, the simulation helps to better understand how the Ethereum network behaves under the proposed circumstances. Performance evaluated includes the load the Ethereum pushes over the infrastructure, the response time under the security threats, and the computing resources utilized by the blockchain. Finally, the recreation of a real-world network attack could help to determine the limitations, weaknesses, and strengths of the proposed framework.

Besides the metrics proposed for the previous sections, availability on the target is also collected. The performance data from both implementations undergo statistical analyses to determine whether statistically significant differences exist in terms of network and computer resource utilization.

Therefore, the following testing scenarios are proposed. The first scenario is to test network performance. The baseline is laid out by the collection of data under "normal" circumstances where network attacks are not deployed. The usually internet and operational traffic is generated with a random traffic generator script, with no blockchain interactions involved. The second scenario is to test Etehreum network performance. It includes the same characteristics described in the first scenario. In addition, all blockchain exchange that includes the CTI information available is added to the same random traffic generator by using the same random seed value. The last scenario simulates distributed attacks to a specific target by gradually injecting network bursts to the target. The same metrics and instruments are used as in the previous scenario to test the security capabilities of the framework and the benefits of a decentralized CTI network. In the end, the first two scenarios are compared based on the criteria listed previously to determine whether the proposal is sustainable. The data collected in the last portion of the experiment should provide the evidence to sustain the security capabilities that in theory, the framework could contribute to different networks and service levels. The security capabilities could also be examined to lay out limitations and determine grounded expectations for real-world implementations. Figure 4 shows the GNS3 network simulation hosted at the Azure cloud, which is used for all the testing scenarios.

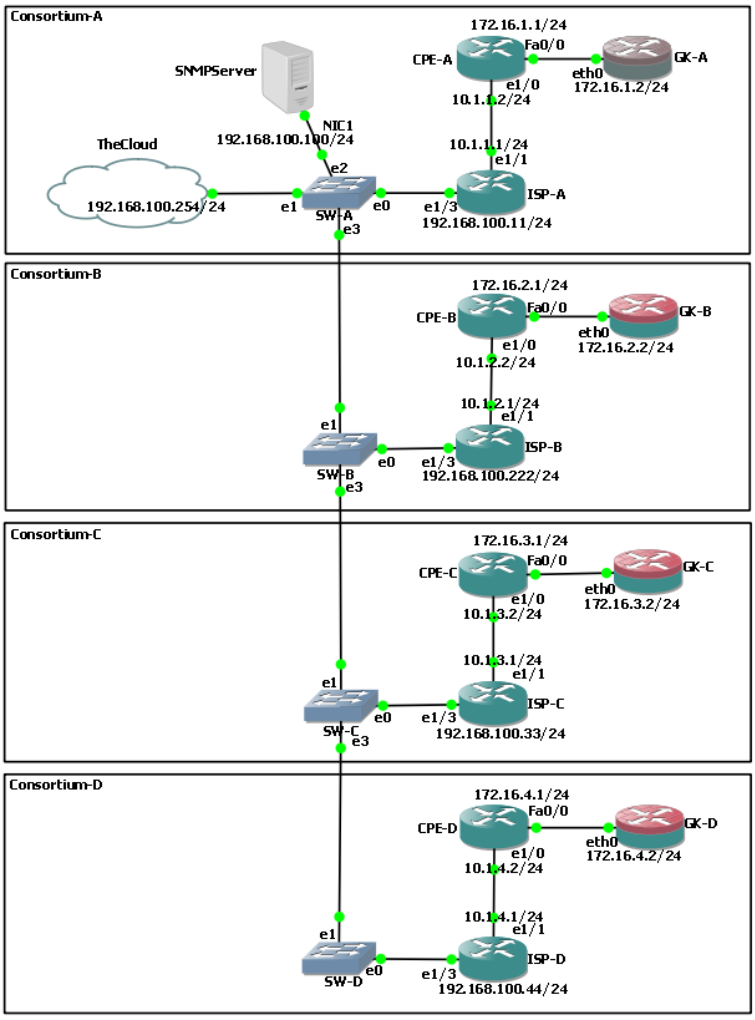

Figure 4. GNS3 network simulation.

Lastly, network performance of video streaming services on the endpoints are also compared between the blockchain-enabled and the conventional network scenarios. Results can be used to examine the differences of user experience, and to determine the viability of the approach at the user level. Both scenarios are set up when the same random network traffic is generated. The data, for this last implementation, are taken directly from the endpoints to compare against the data gathered at the last mile at the ISP level Of the first part of the experiment.

3.2.1. Assumptions

During the experiments, the authors assume all the devices work as expected; the network is designed and implemented correctly; and the network devices encountered no issues other than the problems specifically designed for each testing scenario. Additionally, it is assumed that all blockchain parties behave correctly under the rules and algorithms determined by the Ethereum protocol. Put differently, this work assumes that more than half of the users are legitimate.

3.2.2. Limitations

As the Proof-of-Concept (PoC) is implemented on a consortium Ethereum network, its security relies on a limited number of transaction nodes and validators. In this study, only the authors have access to the Ethereum private network. For the sake of simplicity, the implementation of these smart contracts has not been hardened to the extreme. Only basic secure operations, such as access control, permission controlled were realized during the experiments. And the implementation of the gatekeeper only examined Open System Interconnection (OSI) layer three information, which can be bypassed by attacks that are not included in the threat model of this work.

4. Results

The cloud-based simulation, network diagram shown in Figure 4, ran for fourteen days. The first seven days were used as a "Control" group, where no blockchain instances were included. All blockchain and security implementations were put in place for the rest seven days, which is referenced as the 'Experimental' group in this manuscript. The data was collected via the Simple Network Management Protocol (SNMP), configured at the ISPs' and the customers' premises routers. In total, over 66,000 equally distributed samples entries were collected and the parameters to be analyzed, including Bandwidth (Table 1), CPU utilization (Table 2), and Response Time (Table 3). To recreate network traffic at the user level, a random web traffic generator was used with the same random seed value for the Control and Experimental setups.

The statistics shown in Tables 1–3 show comparisons between the "Control" (no blockchain instances included) and the "Experimental" group (blockchain instances included). The mean, standard deviation (σ_n), and the p-value of the t-test are calculated and listed in the tables for the devices in Figure 4 during the course of experiments. The values presented under the columns labeled Control (C) and Experimental (E) show the mean values of each device. Table 4 shows also a statistical comparison for YouTube streaming performance between the Experimental and the Control groups. Finally, Table 5 pertains to the Experimental group only because blockchain data was only available during this part of the experiment.

Table 1. Mean and standard deviation for utilized bandwidth on routers (Kbps).

Device	Control (C)	σ_1	Experimental (E)	σ_2	p-Value (H_0:$C = E$)
ISP A	93,911.1	561,846	41,443.9	125,030	0.0001
ISP B	148,817	427,260	77,338.0	236,503	0.0001
ISP C	141,282	525,158	84,225.6	381,451	0.0001
ISP D	138,587	326,974	86,659.6	395,937	0.0001

Table 2. Mean and standard deviation for CPU utilization on routers (%).

Device	Control (C)	σ_1	Experimental (E)	σ_2	p-Value (H_0:$C = E$)
ISP A	7.1170	0.5006	5.9493	0.8178	0.0001
ISP B	10.0074	0.6429	8.8812	1.0412	0.0001
ISP C	9.3924	0.6639	8.3844	0.9352	0.0001
ISP D	8.9934	0.6809	8.4193	0.9244	0.0001
CPE A	0.7047	0.7238	1.4948	0.7455	0.0001
CPE B	2.1427	0.3847	2.0402	0.2254	0.0001
CPE C	2.1498	0.3972	2.0497	0.2758	0.0001
CPE D	1.1416	0.4732	1.6144	0.6150	0.0001

Table 3. Mean and standard deviation for response time on routers (ms).

Device	Control (C)	σ_1	Experimental (E)	σ_2	p-Value (H_0:$C = E$)
ISP A	6.5536	3.0634	6.5534	3.1351	0.9965
ISP B	6.4850	3.1223	6.6552	3.1151	0.0005
ISP C	6.6789	3.1686	6.7461	3.1357	0.1720
ISP D	6.6051	3.1133	6.7355	3.1440	0.0077
CPE A	18.0294	5.3292	18.3166	5.3124	0.0006
CPE B	18.1483	5.2870	18.3320	5.3395	0.0270
CPE C	18.5355	5.3244	18.5856	5.3603	0.5491
CPE D	18.4437	5.3562	18.5881	5.2901	0.2094

Because the two testing scenarios are independent, a two-sample t-test was performed to make a comparison with a 95% confidence level [40]. The parameters used for statistical comparison are bandwidth, CPU utilization, and response time.

Table 4. YouTube streaming performance comparison.

Parameter	Control (C)	σ_1	Experimental (E)	σ_2	p-Value (H_0:$C = E$)
Frames Dropped	136.1	61.9451	300.6	128.3	0.0001
Resolution	640 × 360@25	-	640 × 360@25	-	N/A
Connection Speed	12,831.2 Kbps	2962.7	9827.4 Kbps	3711.5	0.0027
Buffer Health	120.9 s	6.7602	121.3 s	9.7353	0.8375

The samples taken from the Microsoft Azure portal for the Ethereum consortium blockchain service include much relevant information of the blockchains. Some key metrics are Block propagation through the network of validators, block creation time, Remote Procedure Call (RPC) traffic, and the usage of CPU, RAM, and disk at the same validator level (Table 5). The data include over 10,000 block metadata collected over seven days. In addition, Netflow data was gathered at the workstations to validate RPC requests and actual traffic generated at the blockchain-enabled CTI enforcement equipment.

Table 5. Blockchain data taken from consortium validators hosted in Microsoft Azure cloud platform.

Parameter	Mean	$\overline{\sigma}$	Unit
Block Propagation	327.0002	96.2419	ms
Block Creation Time	4.4586	1.9444	s
Daily RPC Traffic	0.9638	0.7663	MB
Validator CPU Usage	36.9991	1.1185	%
Validator Available RAM	44.3309	3.0810	%
Validator Disk Usage	13.3417	0.3203	%

Regarding the security features of the PoC, Figure 5 shows the snort alert that signals the presence of multiple ICMP packets trying to reach the target in a short period of time. The snort-enabled device triggered a blockchain transaction, which is recorded by the governing smart contract. The transaction is then broadcast to the rest of the network on the possibility of an ongoing DDoS attack. After a vetting process, the CTI data reached all the subscribed nodes. Actionable events are then triggered. In this case, the firewall of the system, which is IPTables in our experiments, is revised by adding rules to prevent the incoming malicious traffic from transmitting to its destination. The end results were that the automated action slowed or stopped the ongoing DDoS attacks from populating to the downstream networks. Figure 6 shows how the network behaved after blockchain-enabled controls were placed. It visualizes how transmitted and received packets differ in their behaviors. To avoid service outage, the authors limited the number of ICMP packets per second during the attack simulation such that all the necessary data could be properly collected.

Figure 5. (**left**) Snort security event alert. (**right**) Blockchain transactions triggered by the alert.

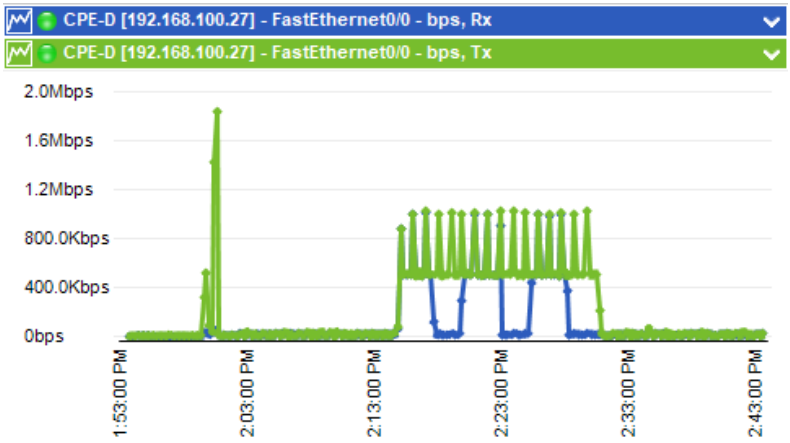

Figure 6. Router interface of target host, received and transmitted packets.

5. Discussion

Data collected at the ISP and the costumer premises equipment (CPE) routers showed a statistically significant difference on bandwidth and CPU utilization. Counter-intuitively, the Control group had greater mean values than the Experimental group, despite the fact that the Experimental group carried an additional load of blockchain information. Further analyses showed that the Control group had a much greater standard deviation, indicating the differences between the samples were much greater than that of the Experimental group. The traffic carried by the Control group was normal traffic and attack traffic, whereas the traffic carried by the Experimental group was normal traffic, blockchain transactions, and reduced attack traffic due to automated deny entries in the IPTables. Results proved that blockchain-based CTI services enabled easier identification of DDoS attacks and faster responses of those attacks. It not only saved network bandwidth but also reduced unnecessary CPU clock cycles for the ISPs to process the DDoS traffic. On the other hand, the CPU utilization of the Experimental group was higher at the edge of

the home network because the additional burden of processing blockchain transactions outweighed the benefits of reduced traffic for each individual home routers. However, the increases in CPU utilization were manageable: none of the Experimental group consumed more than 10% of the CPU resources than the Control group. Regarding response time, only two routers showed statistically significant differences. The Experimental group had a fraction of longer delay than the control group. This suggested that the introduction of the blockchain networks did slow down the network response time for some home networks. The good news was the delay in responses was marginal: merely 2% higher was found in our study.

To understand how the blockchain-enabled security methods impact the end-users on streaming services, YouTube video experiments were implemented. Results showed a slight degradation for the Experimental group. The number of frames dropped and connection speed showed statistically significant differences, favoring the Control setup. However, the buffer health results did not show any statistical differences between the two groups, suggesting that no real visual differences were spotted from the perspective of user experience. This can be further confirmed by the results of video resolutions: both groups automatically played back the video at 640 pixels by 360 pixels, with frame rates of 25 frames/s.

From the blockchain side, the amount of additional traffic originated from daily Ethereum transactions (RPC traffic) is trivial, which did not interfere with normal ISP or user-related operations. Results from these experiments also showed that off-the-shelf hardware was more than sufficient to power the computing needs of the validators. The CPU, RAM, and disk utilization showed no signs of resource starvation. Even if the computing resource becomes a concern to support permissioned blockchains, the consortium scheme will allow additional resources to be dynamically and automatically allocated in the cloud without human intervention.

During the DDoS attack simulation, alerts were immediately triggered by the IDS when the ICMP packets were trying to flood the entire network. Real-time alerts generated real-time blockchain transactions, which activated quick block preparation and subsequent propagation. In fact, the average block creation time was 4.4586 s in our experiment. This means once a DDoS attack was identified by a participating node through Snort signature matching, it took less than five seconds to submit the report to the blockchain by writing the attack information into the data portion of the block. After the block was created, the local node replicated the validated result to the rest of the blockchain network in 0.327 s. This indicates that the CTI report could reach all the participating nodes in the Ethereum network in five seconds from the time the attack was spotted. Such a speedy information creation and propagation would allow users and service providers to enforce security policies in a timely manner when a threat was manifested by the attackers. In a nutshell, the proposed framework demonstrated that integrity-proof, reliable, and relevant data can be shared over a network that does not have centralized trust. The design of the framework met the CTI requirements stated in References [28–30].

By leveraging blockchain, this work can securely share critical information immutably without the need of centralized trust entity. In addition, the proposed approach is designed to interact with the Ethereum network to automatically trigger the defense when known attacks are recognized. The automation process eliminated the need for human intervention and hence reduced the human errors during the incident handling. The automation also helped to streamline the incident response process by providing flexible governing smart contracts. Because the underlying blockchain allows equal access from all the participants, it removed the risk of a single point of failure and improved the overall resilience of the CTI sharing network. Besides these great features, the proposed model also offers fast and lightweight first-hand information sharing. The result is that any participating nodes can augment the threat intelligence in real-time without taking too much toll on the computing resources. During a botnet outbreak, known bad IP addresses and port numbers would not be allowed to transmit during the botnet propagation phase. In other

words, an attack with known characteristics would not succeed in the proposed framework. An unknown attack could still temporarily succeed until the signature of such malicious traffic is identified. During the communication and activity stages, assuming the initial infection has succeeded, the malicious traffic is expected to flow from internal to external sources. If timely information is shared in the CTI, then the malicious traffic can be stopped at the source. This will prevent the external nodes from resource exhaustion and maintain normal network operations. Figure 7 depicts a typical botnet infection stages when an enforcement device is part of the proposed solution.

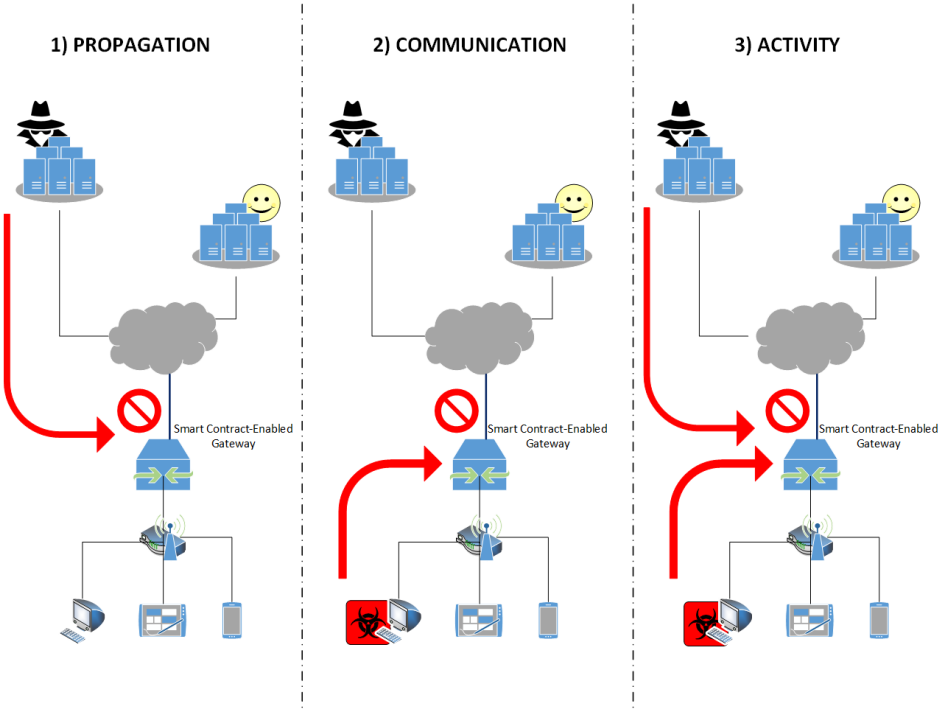

Figure 7. Cyber threat intelligence (CTI) enforcing diagram during three stages of a botnet attack.

6. Conclusions

To safeguard IoT devices for the consumer market, this work investigated a blockchain-enabled CTI sharing network using a distributed data collection method. Simulation results show the proposed framework is viable for normal network load, including randomly generated traffic, as well as typical YouTube streaming services. This suggests when connecting a democratic, immutable, resilient, and secure blockchain network to an actionable cyber threat intelligence system, it can provide a realistic solution to protect ISP infrastructure, home network devices, and home-based IoT devices without a centralized trust entity. The proposed framework is sustainable and scalable because the underlying PoA consortium blockchain service can be executed in the cloud. The tamper-proof property of the blockchain offers an additional layer of protection and prevents nefarious actors from manipulating the CTI data. Because the first-hand CTI information can be augmented and accessed by all the stakeholders, our decentralized CTI system is capable of addressing many CTI challenges observed by large organizations, small businesses, and home consumers. The implementation of permissioned blockchains requires minimal network architectural changes for both the ISPs and the home networks. It can be easily deployed as an added-on service to benefit both parties. In short, the presented approach is a good starting point to a decentralized and actionable CTI system. It can be served as a secure architecture model to protect home networks and IoT devices, as well as critical network infrastructures.

Further study is needed to understand how the 'intelligence' of a single node can be leveraged to improve the overall 'intelligence' of the entire CTI system. In particular,

how a novel attack can be quickly recognized and reliably populated to the rest of the CTI system remains a very challenging task. Additional studies are also needed to understand how the performance degrades when the size of the blockchain gets much bigger and the network traffic gets much heavier. Finally, CTI systems can be more effective when multiple blockchain networks are sharing information with each other. Cross-chain real-time validation can be an intriguing work to greatly improve the impact of the proposed framework.

Author Contributions: D.M.M. conceived, designed, and performed the experiments, analyzed the data and wrote the article's first draft. B.Y. conceived the experiments, provided the methodology, provided the resources and validated the methods, and reviewed and edited the last version of the article. All authors have read and agreed to the published version of the manuscript

Funding: This work is partially supported by the Purdue Polytechnic Institute HSS Seed Grant.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the author.

Acknowledgments: The authors thank Purdue University's Computer and Information Technology Department for their assistance.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

C&C	Command and Control
CPE	Costumer Premises Equipment
CPU	Central Processing Unit
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DNS	Domain Name System
GRE	General Routing Encapsulation
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IOC	Indicator of Compromise
IoT	Internet of Things
ISP	Internet Service Provider
PoC	Proof of Concept
SNMP	Simple Network Management Protocol
TCP	Transfer control Protocol
RAM	Random Access Memory

References

1. Mendez Mena, D.; Papapanagiotou, I.; Yang, B. Internet of things: Survey on security. *Inf. Secur. J. Glob. Perspect.* **2018**, *27*, 162–182. [CrossRef]
2. Krebs, B. DDoS on Dyn Impacts Twitter, Spotify, Reddit. Available online: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/ (accessed on 29 December 2020).
3. Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6. [CrossRef]
4. Mendez Mena, D.; Yang, B. Blockchain-Based Whitelisting for Consumer IoT Devices and Home Networks. In Proceedings of the 19th Annual SIG Conference on Information Technology Education, SIGITE'18, Fort Lauderdale, FL, USA, 3–6 October 2018; ACM: New York, NY, USA, 2018; pp. 7–12. [CrossRef]
5. Bertino, E.; Islam, N. Botnets and internet of things security. *Computer* **2017**, *50*, 76–79. [CrossRef]
6. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]

7. Cui, A.; Stolfo, S.J. A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan. In Proceedings of the 26th Annual Computer Security Applications Conference, Austin, TX, USA, 6–10 December 2010; pp. 97–106.
8. Karamanos, E. Investigation of Home Router Security. Master's Thesis, KTH Information and Communication Technology, Stockholm, Sweden, 2010.
9. Yiakoumis, Y.; Yap, K.K.; Katti, S.; Parulkar, G.; McKeown, N. Slicing home networks. In Proceedings of the 2nd ACM SIGCOMM Workshop on Home Networks, Toronto, ON, Canada, 15–19 August 2011; pp. 1–6. [CrossRef]
10. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341. [CrossRef]
11. Lohachab, A.; Karambir, B. Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks. *J. Commun. Inf. Netw.* **2018**, *3*, 57–78. [CrossRef]
12. Zhang, Z.K.; Cho, M.C.Y.; Wang, C.W.; Hsu, C.W.; Chen, C.K.; Shieh, S. IoT Security: Ongoing Challenges and Research Opportunities. In Proceedings of the 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, 17–19 November 2014; pp. 230–234. [CrossRef]
13. Pacheco, J.; Hariri, S. IoT Security Framework for Smart Cyber Infrastructures. In Proceedings of the 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), Augsburg, Germany, 12–16 September 2016; pp. 242–247. [CrossRef]
14. Yu, T.; Sekar, V.; Seshan, S.; Agarwal, Y.; Xu, C. Handling a trillion (unfixable) flaws on a billion devices. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets-XIV), Philadelphia, PA, USA, 16–17 November 2015; ACM Press: New York, NY, USA, 2015; pp. 1–7. [CrossRef]
15. Oracevic, A.; Dilek, S.; Ozdemir, S. Security in internet of things: A survey. In Proceedings of the 2017 International Symposium on Networks, Computers and Communications (ISNCC), Marrakech, Morocco, 16–18 May 2017; pp. 1–6. [CrossRef]
16. Luu, L.; Chu, D.H.; Olickel, H.; Saxena, P.; Hobor, A. Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 254–269.
17. Shrier, D.; Wu, W.; Pentland, A. Blockchain & Infrastructure (Identity, Data Security). Technical Report, Retrieved 27-11-16. Available online: http://cdn.resources.getsmarter.ac/wp-content/uploads/2016/06/MIT_Blockain_Whitepaper_PartThree.pdf (accessed on 19 August 2016).
18. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
19. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
20. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
21. Jasper, S.E. U.S. Cyber Threat Intelligence Sharing Frameworks. *Int. J. Intell. CounterIntell.* **2017**, *30*, 53–65. [CrossRef]
22. Wagner, C.; Dulaunoy, A.; Wagener, G.; Iklody, A. MISP—The design and implementation of a collaborative threat intelligence sharing platform. In *WISCS 2016-Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, Co-Located with CCS 2016*; Association for Computing Machinery, Inc.: New York, NY, USA, 2016; pp. 49–56. [CrossRef]
23. Cha, J.; Singh, S.K.; Pan, Y.; Park, J.H. Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing. *Sustainability* **2020**, *12*, 6401. [CrossRef]
24. Yan, Z.; Kantola, R.; Shen, Y. Unwanted traffic control via global trust management. In Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, China, 16–18 November 2011; pp. 647–654. [CrossRef]
25. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Blockchain with Internet of Things: benefits, challenges, and future directions. *Intell. Syst. Appl.* **2018**, *6*, 40–48. [CrossRef]
26. Ølnes, S.; Ubacht, J.; Janssen, M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Gov. Inf. Q.* **2017**, *34*, 355–364. [CrossRef]
27. Hughes, L.; Dwivedi, Y.K.; Misra, S.K.; Rana, N.P.; Raghavan, V.; Akella, V. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *Int. J. Inf. Manag.* **2019**, *49*, 114–129. [CrossRef]
28. Al-Ibrahim, O.; Mohaisen, A.; Kamhoua, C.; Kwiat, K.; Njilla, L. Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligence. *arXiv* **2017**, arXiv:1702.00552.
29. Böhm, F.; Menges, F.; Pernul, G. Graph-based visual analytics for cyber threat intelligence. *Cybersecurity* **2018**, *1*, 1–19. [CrossRef]
30. Mtsweni, J.; Mutemwa, M. Technical Guidelines for Evaluating and Selecting Data Sources for Cybersecurity Threat Intelligence. In Proceedings of the ECCWS 2019 18th European Conference on Cyber Warfare and Security, Coimbra, Portugal, 4–5 July 2019; pp. 305–313.
31. Berndt, A.; Ophoff, J. Exploring the Value of a Cyber Threat Intelligence Function in an Organization. In *IFIP Advances in Information and Communication Technology*; Springer Science and Business Media Deutschland GmbH: Berlin/Heidelberg, Germany, 2020; Volume 579, pp. 96–109. [CrossRef]
32. Li, V.G.; Dunn, M.; Pearce, P.; McCoy, D.; Voelker, G.M.; Savage, S.; Levchenko, K. Reading the tea leaves: A comparative analysis of threat intelligence. In Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, 14–16 August 2019; pp. 851–867.

33. Abu, S.; Selamat, S.R.; Ariffin, A.; Yusof, R. Cyber Threat Intelligence-Issue and Challenges. *Indones. J. Electr. Eng. Comput. Sci.* **2018**, *10*, 371–379. [CrossRef]
34. Atzori, M. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? *SSRN Electron. J.* **2016**. [CrossRef]
35. Wu, Y.; Qiao, Y.; Ye, Y.; Lee, B. Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing. In Proceedings of the 2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS, Granada, Spain, 22–25 October 2019; pp. 474–481. [CrossRef]
36. Buber, E.; Sahingoz, O.K. Blockchain Based Information Sharing Mechanism for Cyber Threat Intelligence. *Balk. J. Electr. Comput. Eng.* **2020**, *8*, 242–253. [CrossRef]
37. Hajizadeh, M.; Afraz, N.; Ruffini, M.; Bauschert, T. Collaborative cyber attack defense in SDN networks using blockchain technology. In Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridging the Gap Between AI and Network Softwarization, NetSoft 2020, Ghent, Belgium, 30 June–3 July 2020; pp. 487–492. [CrossRef]
38. Purohit, S.; Calyam, P.; Wang, S.; Yempalla, R.K.; Varghese, J. DefenseChain, Consortium Blockchain for Cyber Threat Intelligence Sharing and Defense. In Proceedings of the 2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020; pp. 112–119. [CrossRef]
39. Shani, T. Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important. Available online: https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/ (accessed on 10 September 2020).
40. Devore, J.L. *Probability and Statistics for Engineering and the Sciences*; Cengage Learning: Boston, MA, USA, 2011; ISBN: 978-1305251809.