Blockchain-based frameworks for mitigating DDoS and Sybil attacks in the IoT

Author: Cemal Dikmen[1] **, Supervisor: Miray Ayşen**[1] **, Responsible Professor: Dr. Zekeriya Erkin**[1]

Cyber Security Group CSE3000 Research Project
Department of Intelligent Systems
[1]Delft University of Technology
c.dikmen@student.tudelft.nl, {z.erkin, m.aysen}@tudelft.nl

Abstract

With the growing scale of the IoT, many industries enjoy the benefit of automation. The IoT consists of an interconnected network of devices that sense their surroundings and share data among other IoT devices. However, this data can be sensitive and private in nature, making security within the ever-growing IoT network a high priority. Because of the constrained nature of IoT devices, namely limited computing power, memory and energy, classical cryptographic solutions are not desired. Furthermore, current IoT frameworks are heavily centralised around central servers which can result in single points of failure in the case of DoS attacks. Because of these drawbacks, the emerging blockchain technology is seen as a potential solution to these problems. A blockchain is a distributed ledger that is able to keep an immutable list of transactions occurring in a network. The purpose of this research is to compare blockchain-based frameworks for mitigating DDoS and Sybil attacks in the IoT by comparing proposed blockchain-based frameworks. Qualitative evaluation of proposed frameworks suggests that there are several strategies to improve security within the IoT. Blockchain, in addition to other technologies such as SDN, can provide effective mitigation of DDoS attacks and Sybil attacks. However, there is limited quantitative test data available and further research is required in this novel field of research.

1 Introduction

In October 2016, the Mirai botnet, which consisted of an incredible amount of IoT devices, conducted a devastating distributed denial of service (DDoS) attack by targeting Dyn, a popular DNS provider. Resulting in over 600k infected devices, the attack with a magnitude exceeding 1.2 Tbit/s is one of the largest of its kind to this day [1]. This attack overwhelmed multiple high-end websites and services that used Dyn as their DNS provider, such as Amazon, twitter, GitHub and PayPal, causing them to be unreachable for several hours [2]. With a constantly growing IoT network, attacks such as the Mirai botnet can become larger and more devastating which emphasises the importance of security in IoT devices [2], [3].

Current IoT frameworks are heavily centralised around large central servers and this has direct consequences in security, privacy and scalability of the IoT [4]. In the case of a denial of service (DoS) attack, the central servers can be paralysed which result in single points of failure. Furthermore, these servers are controlled by third-parties and the particular parties need to be trusted by users for the treatment of their data. Moreover, this centralised approach results in a higher latency as the IoT network keeps growing and this limits the application of the IoT in settings such as smart cities [5], [6]. The problems with centralised frameworks can be summarised by the following points:

- Central servers can form single points of failure.
- Third parties need to be trusted with private IoT data.
- The scalability of the growing IoT network is limited.

As the IoT is continually growing, recent literature has seen emerging technologies such as Software Defined Networking (SDN) and decentralised approaches such as blockchain and Directed Acyclic Graphs (DAGs) as promising solutions for IoT privacy and security issues [7], [8], [9], [10]. This is because SDN allows for more programmability within the network, resulting in a more manageable IoT network as the IoT keeps increasing in size and complexity. Furthermore, a decentralised approach removes the single points of failure, eliminating the reliance on central servers and resulting in a more robust and secure infrastructure [11]. Peers in the blockchain network can verify the data integrity and the identity of the sending devices. This consensus makes the distributed ledger fault tolerant. Third parties controlling current centralised servers need to be trusted for data handling. Thus having no third party at hand increases privacy and trust in the system [5]. Moreover, smart contracts can provide increased security in the form of programmable contract rules that are enforced during every transaction [12].

Because of the ever-growing network of the IoT and IoT devices having specific tasks and are usually heavily constrained devices incapable or running state-of-the-art security protocols, IoT devices are increasingly becoming a tool for DDoS attacks and these attacks have increased in scale enormously [13], [14].

Contributions

In this paper, the aim is to highlight blockchain-based solutions to two different security attacks that are the result of current IoT security issues, namely DDoS attacks and Sybil attacks. Different decentralised solutions will be compared to each other and recommendations and advice will be given on the proposed frameworks and future research.

The main contributions of this research are as follows:

- We highlight important security challenges and drawbacks of current IoT frameworks.
- We show the benefits of a decentralised approach in resolving centralised problems.
- We present a comparison between proposed blockchain-based security frameworks.
- Finally, we give recommendations and advice for future research.

The paper is organised as follows. Section 2 provides a short overview of related work. Section 3 explains the methodology used. Section 4 gives background information regarding the IoT and its security risks, followed by an explanation of blockchain technology and its benefits. SDN is also explained as well as both DDoS attacks and Sybil attacks. Section 5 provides the analysis part in which several proposed blockchain-based frameworks are analysed. Section 6 gives the comparison of these frameworks based on the technologies used. Section 7 provides a discussion of the results found and suggests future work. Section 8 covers the ethical aspects of this research and discusses the reproducibility. Finally, section 9 concludes the paper.

2 Related Work

Due to the increasing size of the IoT and popularity of blockchain, blockchain is a popular choice to address challenges in IoT settings such as security, privacy and trust. Researchers have looked into these proposed solutions and provided survey articles to compare them in different settings. However, the literature is limited with regards to the comparison of blockchain-based framework in the mitigation of cyber attacks in IoT settings.

Ali *et al.* [5] provide a comprehensive survey of blockchain-based frameworks for the IoT. General challenges such as security, privacy and trust have been addressed and frameworks trying to solve some of these challenges are compared. Sengupta *et al.* [10] provide an extensive survey on attacks and security issues in both the IoT and Industrial IoT (IIoT). They provide a taxonomy of security attacks on the IoT and highlight several centralised solutions. Finally, they explain how blockchain can be a solution to IoT and IIoT security issues in general, without highlighting blockchain-based frameworks.

Kshetri [15] and Khan and Salah [16] give an overview of IoT security issues and how blockchain can help improving IoT security without going in-depth or comparing specific blockchain-based frameworks. Minoli and Occhiogrosso [17] highlight the use of blockchain mechanisms for improved security in certain IoT settings without comparing the mechanisms or portraying frameworks that incorporate these mechanisms to improve IoT security.

To the best of our knowledge, there are no papers in the literature specifically looking into how blockchain-based security frameworks can mitigate web attacks such as DDoS attacks and Sybil attacks. Therefore, this paper is aiming to start filling the gap in research and provide a comparison of the limited amount of proposed blockchain-based frameworks for the mitigation of DDoS attacks and Sybil attacks.

3 Methodology

For this literature study, blockchain-based IoT security frameworks are being compared in the context of mitigating both DDoS attacks and Sybil attacks. Background information regarding the problem statement and introduction of blockchain-based IoT frameworks are inspired by [5]. The authors provided a comprehensive survey regarding blockchain in the IoT, highlighting various issues within the IoT and presenting proposed blockchain-based solutions for these issues. To investigate various proposed solutions for specifically DDoS and Sybil attacks, Google Scholar, Web of Science and Scopus were used. The search terms used for this investigation were: “Blockchain AND IoT AND DDoS”, “Blockchain AND IoT AND Sybil”, “Blockchain AND IoT AND Security”.

The comparison is of qualitative nature as most papers of proposed solutions do not provide quantitative test results. The different technologies used are addressed and compared in the IoT setting.

4 Background

In this section, both the Internet of Things (IoT) and blockchain technology are introduced and explained. Before looking at the integration and applications of blockchain in the IoT, the features of blockchain technology are important to understand in order to realise its benefits in the IoT.

4.1 The Internet of Things

Recently, in 2015, the IEEE IoT Initiative aimed to establish a sound definition of the Internet of Things (IoT) which ranges from smaller systems and devices restricted to distinct locations to a larger global system that is distributed to more sub-systems [18].

The Internet of Things is the name for a novel concept in which various objects are embedded in the environments around humans, such as radio-frequency identification (RFID) tags, sensors, actuators, etc., that communicate and collaborate with each other in order to aid humans by means of automation [19], [20]. These objects, or things, gather tremendous amounts of data from their surroundings and interact with each other and with the physical world while using existing Internet standards to provide services for information transfer, analyticsm applications and communications [21]. These objects are applied in several real-world settings and the applications can be found in domains such as transportation and logistics, healthcare, the smart environments (home, office, plant) and personal and social environments [19].

However, data collected by these interconnected devices may contain private and sensitive information. With the collection of large amounts of private data, both security and privacy concerns naturally arise [20]. Moreover, IoT networks are deployed on so-called low-power and lossy networks (LLN). These LLNs are networks that have limited energy, memory and processing power to utilise, resulting in the lack of comprehensive cryptographic security algorithms and mechanisms [20].

Conventional networks, depending on the application, do not have the constraints caused by the nature of the deployment of IoT networks on LLNs. These constraints can lead to severe security compromises in the IoT. If an attacker can join the network assuming any identity, it can be seen as an authentic node in the network. This results in data collection being manipulated and wrong control messages being sent as a result [20]. Furthermore, existing security mechanisms are not applicable because of the highly constrained nature of IoT devices in terms of computing power, memory and energy [22].

A crucial security complication stems from the expanding IoT edge. In IoT networks, edge devices are recently joined devices with limited memory, processing power and outdated operating systems [23]. These devices are thus easily compromised and can form botnets to disintegrate the IoT network itself or other targets [5], [23].

4.2 Blockchain technology

Blockchain technology is becoming more popular in the media since the rise of various cryptocurrencies, such as Bitcoin [24]. These cryptocurrencies are utilising important features of blockchain technology, but they are merely one of the many applications possible with blockchain [25].

A blockchain is a distributed ledger that keeps track of transactions in a network. Each block of the network has a copy of all information of previous transactions made. Transactions can be seen data exchanges or cryptocurrency payments, for example. As the name implies, a blockchain is a chain of blocks in a network where each block contains some information. A block can be compared to the structure of a network packet: it has a header and a body. The header of a block contains the identifier which is a cryptographic hash that is calculated based on the contents of the body of the block. Alongside this hash, the header also contains the cryptographic hash of the previous block. If someone were to modify information in a block, its cryptographic hash would be different. This means that the next block now has a different hash stored than the modified block's hash resembles, making the modified block invalid. A hacker would only succeed if he/she could alter headers in the majority of all subsequent blocks, creating a consensus, which is nearly impossible to do [12]. This important feature results in data being immutable in the blockchain and is one of the most important security advantages of blockchain technology [26]. Therefore, many applications use blockchain as a basis in order to provide decentralised solutions [25].

To maintain consensus, the ledger needs to be updated and distributed among all peers in the blockchain network. Consensus algorithms try to do this securely. Because of the distributed nature of blockchain and its consensus algorithms, blockchain is fully decentralised. This means that there is no central point of authority in any stage and is regarded as one of the most important aspects of its security and privacy features [5].

Another aspects of blockchain technology comes in the form of smart contracts. These contracts consist of contractual clauses translated into code that can enforce them, without the need for trusted intermediaries [12]. These contracts are scripts stored on the blockchain that are run when a transaction is addressed to it, following an execution of the smart contract on every block in the chain.

4.3 Software Defined Networking

As computer networks continuously grow larger in size and complexity, Software Defined Networking (SDN) is seen as a solution to ease network maintenance and network management [27], [28]. Both the process of integrating policies and changing existing policies, as a result of weaknesses in the network, is complicated. SDN separates the control logic from the data management and introduces progammability which allows for accessible maintenance of the network. Hence, both network management and expansion of the network is uncomplicated [28]. Because of this decoupling of the data plane and control plane, more freedom is granted in controlling the network and dealing with network attacks such as DDoS [29], [30], [28].

4.4 Sybil and DDoS Attacks

Sybil attacks

In Sybil attacks, adversaries can replicate multiple bogus identities that appear to act legitimately, while at the same time performing malicious actions within the network. These devices with fake identities are called Sybils. The presence of Sybils in the blockchain is especially concerning because of the nature of blockchain consensus mechanisms. In these consensus mechanisms, 51% of peers need to confirm a transaction before it becomes valid and is added to the blockchain [31]. If Sybils comprise more than 51% of the network, the blockchain's data integrity and security will be compromised as this can lead a variety of attacks on the network and from the network, such as DDoS attacks [32], [33].

DDoS attacks

The goal of a denial of service attack is to limit or deny the ability of users gain access to a service. This is realised by consuming resources linked to that particular service, such as bandwidth [34]. As a result, users are denied access to the service. Distributed denial of service attacks are a more advanced form of dos attacks in which numerous nodes or entities are involved in realising the denial of service. In the context of the IoT, the many constrained devices can be compromised to conduct a DDoS attack [13].

5 Analysis

In this section, multiple blockchain-based IoT security frameworks are highlighted with particular emphasis on either DDoS attacks or Sybil attacks. The frameworks utilise different tools and technologies combined with blockchain, which will be discussed and addressed. The literature regarding DDoS and Sybil mitigation in IoT utilising blockchain technology is limited as this is a new and on-going research topic. The authors of proposed solutions mostly display their architecture and often without implementations or test data. They theoretically analyse the success of their framework based on the salient features of blockchain used for the mitigation of DDoS or Sybil attacks in the context of the IoT.

5.1 Blockchain-based DDoS mitigation in IoT

Co-IoT

Co-IoT is a collaborative blockchain-based framework that utilises SDN to specifically mitigate DDoS attacks within an IoT environment [35]. The main idea of this framework is collecting information of malicious devices using smart contracts and the Ethereum blockchain. The authors argue that collaboration between several Autonomous Systems (ASs) or IoT devices, is necessary in order to mitigate DDoS attacks because these attacks grow rapidly and are becoming more devastating by exploiting and hijacking IoT devices, as can be seen in the Mirai botnet [1], [35].

In the proposed framework, there exist multiple SDN domains which consist of a group of IoT devices. All SDN domains collaboratively create and maintain a list of information of malicious IoT devices that potentially support an ongoing DDoS attack. This information consists of IP-addresses of these malicious devices. Each SDN domain runs an instance of an Ethereum client and the SDN controllers in the SDN control plane transfer attack information in a secure and decentralised manner in the shared ledger using Ethereum smart contracts. Once blocks are mined, which happens every 14 seconds, all authorised IoT devices in other SDN domains have access to the stored information including information regarding the malicious nodes of the network to be blocked.

Co-IoT provides DDoS mitigation while an attack is happening and close to the start of the attack [35]. Hence, it cannot prevent DDoS attacks from happening as the mitigation strategy is focused on detecting attacks and resolving those attacks after having identified them. Another downside is that the framework relies on other mitigation schemes for the detection of malicious behaviour.

Blockchain-based SDN

Giri *et al.* [36] propose a similar solution to Co-IoT in which a smart contract is deployed in a blockchain to enable collaborative DDoS mitigation across SDN domains. Here, IP addresses of malicious devices are reported and stored in the blockchain. Because of the decentralised nature, the entire network of devices has the same information and malicous packets will be dropped. The actual defense mechanism is executed in the SDN using mitigation techniques and

To mitigate DDoS attacks, they use a DDoS security application and a smart contract in parallel where the application monitors the network traffic for traffic that surpasses a predefined maximum-responses count. If a DDoS attack is detected, the network traffic coming from the malicious device is blocked or limited after which the information of the malicious device is added to the blacklisted IP list in the shared ledger after which it is propagated in the network using smart contract. At the same time, the source address of incoming packets will be analysed and checked and if it is conforming to blacklisted IP addresses in the shared ledger, the packets will be dropped [36].

A layered framework

An interesting view on the matter is provided by the framework of Shafi and Basit [37]. The authors look at the problem of both defending an IoT network from DDoS attacks as well as preventing the IoT network of becoming part of a botnet capable of launching DDoS attacks. The layered architecture utilises both SDN and blockchain to achieve this and the framework consists of two modules with each having different tasks ranging from preventing the creation of botnets, to mitigating DDoS attacks [37].

The first layer is called the Log Module. The purpose of this module is to prevent 'innocent' devices from becoming part of a botnet. It analyses incoming packets on a set of metrics stored in the shared blockchain ledger for recognising any malicious and suspicious traffic destined for 'innocent' devices. The second layer is called the Security policy Module. This module enforces security policies by flagging IoT devices that meet the preset minimum security standards and storing their data in a list of white listed devices on the shared ledger. This should help the Log Module keeping a closer eye on packets coming from devices that do not meet the minimum security standards. However, the authors do not specify what kind of blockchain they use in their framework.

DDoS prevention framework with gas limits

Javaid *et al.* [38] proposed an Ethereum-based framework to specifically address DDoS attacks in the IoT, replacing centralised IoT infrastructures with a decentralised one.

Their network model consists of several parts, starting with IoT devices which are connected to a gateway. This gateway can be used for communication among a set of devices. Moreover, the smart contract is the brain of the network, it is seen as the 'server', distributed on the blockchain. It regulates authorisation of the devices and ensures that the devices do not go beyond their 'gas limit' by which each transaction is bound. Gas is analogous to resource and it represents the computational power required for different transactions within the Ethereum blockchain. This gas limit is defined in the smart contract and is one of the central parts of this framework in mitigating DDoS attacks. The smart contract allocates the gas limit to each device above which it cannot operate. This limit is based on the specifications and tasks of an IoT device. Furthermore, IoT devices can use the smart contract to send a message. The message will be send via the blockchain and is stored in the distributed ledger for retrieval only if the receiving IoT node is granted access [38].

Additionally, the smart contract has a list of trusted and untrusted IoT devices. If a device calls a function in order to send a message, the identity and authorisation of the device will be checked. If the device is unauthorised, all of its messages will be dropped and disregarded.

Finally, the system consists of multiple miners that have high computational power to verify transactions in the

Ethereum blockchain. An advantage is that they put an emphasise on the integration with so-called 'legacy' IoT devices with extremely low computational power. However, the authors make strong assumptions with the most notable being that DDoS attacks cannot happen on Internet hosts and on the miners themselves [38].

In the case of a DDoS attack, multiple devices in the network are sending exceptionally large amounts of data to overload a server and consume its resources. The gas limit set by the smart contract prevents the system from overloading. The smart contract uses a function in which there are n IoT devices, each having a gas limit of g_i and the maximum bandwidth available is B.

$$\sum_{i=1}^{n} g_i \leq B \tag{1}$$

Equation (1) illustrates that even if all devices will send data at their maximum gas limit at the same time, the maximum bandwidth will not be exhausted.

Hierarchical blockchain approach

Al-Shakran *et al.* [39] have designed a hierarchical botnet prevention model for the IoT using blockchain, smart contracts and SDN in order to mitigate and prevent DDoS attacks. In this framework, the IoT network is seen as multiple network segments. Each network segment comprises a small set of IoT devices and a local storage unit is present to save all transactions. Each network segment also has a local blockchain and a smart contract which contains SDN controllers that hold policies. SDN is used to separate the data plane from the control plane which provides programmability and automation to the network. This customisation is used to enforce security policies with smart contracts in the network. Local blockchains are connected to a global blockchain which contains a global smart contract registry in which each local smart contract needs to register itself. This global blockchain stores the IP addresses of IoT devices and information about their authorisation. The smart contract has a set of rules which the SDN monitors. If an IoT device does not adhere to these rules, it is being blacklisted and its information is stored in the local blockchain and shared to the global blockchain. The global blockchain distributes the IP address of this device to the rest of the connected network segments which they store in the list of untrusted devices. Messages from untrusted or blacklisted IoT devices will be blocked and disregarded.

The advantages of this approach is the abstraction provided. Multiple IoT networks can be connected and secured in this fashion where local blockchains are connected to a global blockchain and the distribution of important information covers multiple network segments. However, the authors do not provide the set of rules that is going to be embedded in the smart contracts and they do not specify the SDN policies. This approach can be combined with previous frameworks to make it more complete and can then be tested with simulation or on constrained physical IoT devices.

5.2 Blockchain-based Sybil mitigation in IoT

Since this is a novel field of research, Sybil resistant blockchain-based IoT frameworks in the literature is extremely limited. This subsection will focus on two approaches of blockchain-based Sybil mitigation in the IoT and will highlight advantages and disadvantages.

In centralised IoT frameworks, devices that are being entered into the network are trusted and authorised from the beginning with a consequence that they are expected to be trusted permanently, therefore trust monitoring approaches and architectures are proposed to resolve this issue [40].

Sybil resistant trust model for the IoT

A Sybil resistant blockchain-based IoT framework established around trust among IoT devices, is proposed by [41]. The framework uses the Hyperledger Fabric blockchain [42]. This blockchain simulates and validates proposed transactions before they are being added to the blockchain ledger. Transactions can be accepted or rejected based on a preset list of rules. This is evaluated by dedicated nodes in the blockchain network, whose purpose is solely evaluating the validity of transactions proposed by IoT devices. Before a transaction is even proposed, the framework evaluates the so-called trust score of the proposing IoT device. This trust score is a rating between 0 and 100 and can be adjusted after each transaction. The adjustment is based on the receiving IoT device which rates the trust score of the serving IoT device based on its packet forwarding behaviour, or packet delivery rate (PDR). The PDR is determined based on the type and functions of the IoT device. The threshold of the minimum allowed trust score is a pre-defined system parameter known to all IoT devices in the network. If the PDR of an IoT device is above a certain value, its trust score will be impacted negatively. Finally, if the trust score is below the system threshold, all messages and data from the IoT device will be dropped and disregarded.

Rechained

Rechained [43] is a Sybil resistant blockchain-based IoT framework. Their main goal is to verify devices in the Rechained IoT network where Internet access can be limited or non-existent as is the case in various IoT settings such as supply chain or vehicular applications. Before devices are part of the Rechained network, they need to be added or created. If an identity already exists outside the Rechained network, the identity is assumed to have a corresponding key pair representing a Bitcoin wallet address. For the creation of an identity for an IoT device, a public and private key pair is used to link IoT device by sending a Bitcoin transaction to a predefined address. Once this transaction is validated by the proof of work (PoW) calculations and added to the blockchain, an identity proof will be created which includes the proof ID of the IoT device and this allows the IoT device to enter the Rechained network. The way in which access is controlled by means of cryptocurrency is called tokenisation. Once devices are part of the network, verifying their identities is critical in preventing Sybil attacks. Before the devices start communicating, verification of identities of peers is needed. To verify an identity, two devices exchange their identity proofs by means of a two-way handshake. The format of the identity proof will be examined on parameters such as the proof ID. Finally, a major drawback in this framework is the use of the Bitcoin blockchain with its computationally heavy PoW consensus mechanism and high volatility [5], [44]. The high volatility can cause transactions to be extremely expensive which is unwanted in an IoT network in which devices are sharing data constantly in the form of transactions.

6 Comparisons and Results

In this section, the found frameworks from section 5 are compared and the technologies used are reflected on. An overview of the different frameworks and their main features, used technologies and limitations can be found in Table 1.

6.1 Challenges and Risks

Aside the brief drawbacks discussed in section 5, fundamental technologies used in certain frameworks, such as SDN, also have significant deficiencies and face several challenges that could hinder the performance, security, resiliency and scalability of the IoT network on which they are applied [45]. The frameworks Co-IoT [35], [36], [37] and [39] all use SDN as a technology in mitigating DDoS attacks. Although the promising benefits discussed which SDN can realise in comparison with traditional networks, SDN has many drawbacks that need to be considered when incorporating the technology in vulnerable and sensitive settings such as the IoT. Indeed, SDN faces several challenges and potential risks. In a comprehensive survey about SDN [28], the authors highlight several challenges and drawbacks of SDN and suggest more research needs to be done.

Resiliency can be a drawback because of the added complexity in the separation of the data plane and control plane and the extra communication needed between the two planes. This separation in architecture can have possible failures in different places, resulting in less fault tolerance and thus decreased resilience [28]. Another problem that arises because of the decoupling of the data and control planes, is scalability [28]. Due to its architecture, the control plane faces increased network load because of additional control plane traffic. This results in potential bottlenecks in large-scale networks [28], which can be a problem in the long-term growth of IoT applications. Lastly, many security risks have been identified in SDNs [45]. Some of these risks are specific to SDN while others are common in conventional networks such as the risk of DDoS attacks. Specific security risks in SDN are also related to its architectural layers. A successful attack on the control plane communication can allow attackers to control the network, with devastating results such as large-scale data theft [45].

Another challenge comes from the choice of specific blockchains used in the frameworks. Co-IoT [35] and [38] both use the Ethereum blockchain in mitigating DDoS attacks. [41] uses the Hyperledger Fabric blockchain and [43] uses the Bitcoin blockchain in mitigating Sybil attacks. Finally, [36], [39] and [37] do not specify a specific blockchain in their DDoS mitigation strategies, only the pertinent featuers of blockchain technology itself are described in formulating their frameworks. Ethereum and Bitcoin are both permissionless blockchains, whereas Hyperledger Fabric is a permissioned blockchain. In permissionless blockchain, anyone can join the network in contrast to permissioned blockchains in which access is restricted to permissioned nodes only [46]. This means that the use of permissionless blockchains requires access control policies embedded in smart contracts in order to improve security with regards to both DDoS attacks and Sybil attacks. On the contrary, Co-IoT [35] uses Ethereum and cannot prevent DDoS attacks from happening and the authors focus on the mitigation of DDoS attacks during the actual attack. Furthermore, Bitcoin and Ethereum have consensus at the ledger level, meaning that all participants can partake in reaching consensus. Hyperledger Fabric has consensus at transaction level which only involving participants of the actual transaction, resulting in better performance [46]. Consensus in Bitcoin and Ethereum is reached in the form of PoW algorithms that are computationally expensive, whereas Fabric has a flexible and adjustable consensus algorithm making it more suitable for IoT settings [47]. Finally, although transactions are anonymised in PoW, records are available to all nodes which raises privacy concerns [46], [47]. This is not the case in Hyperledger Fabric, making it more suitable in settings where privacy concerns are raised such as healthcare and smart cities.

An important advantage of Ethereum is its gas. Gas is representing the amount of computational work required for a transaction. Each transaction has its gas price defined. This is a major benefit in mitigating DDoS attacks as seen in [38], in comparison with Bitcoin that does not have such a cost specification per transaction [48]. As seen in [38], gas can be used to prevent DDoS attacks from happening in an efficient way.

Rechained [43] specifically focuses on IoT access control in which a device is required to proof its identity before accessing the network, resulting in increased trust among devices. Devices need to be trusted throughout their operation in an IoT network in order to mitigate both DDoS attacks and Sybil attacks. However, access control alone is not enough as it limits devices being entered into the network, but fails to ensure that devices in the network are currently trusted. The proposed Sybil mitigation framework from [41] takes care of this issue by having a pointsystem in works where each IoT device has a trust score and based on its activity, the score can be increased or decreased. Other devices elaborate this on certain preset metrics that can be configured. Such a system can be incorporated with DDoS mitigation frameworks to cover both DDoS attacks and Sybil attacks.

Finally, tokenisation has its benefits in both mitigating DDoS attacks and Sybil attacks [5]. This is because everey transaction is link to an exchange in tokens that represent a real monetary value. However, cryptocurrencies are extremely volatile [44]. This can hinder the many transactions happening in an IoT network as data is constantly being shared among devices. One solution for this would be to use a cryptocurrency which retains its value, specifically made for IoT applications.

Table 1: Comparison table of frameworks and their technologies and drawbacks

Framework	**Focus**	**Main features**	**Blockchain**	**Other Technologies**	**Limitations**
Co-IoT [35]	DDoS	Collaboration of IoT devices, blacklisting IPs	Ethereum	SDN, Smart contracts	No DDoS prevention, SDN risks, Ethereum limitations
Giri *et al.* [36]	DDoS	Blacklisting IPs	Unspecified	SDN, Smart contracts	SDN risks, Conventional mitigation techniques
Shafi and Basit [37]	DDoS	Botnet prevention, Whitelisting IPs	Unspecified	SDN	SDN risks
Javaid *et al.* [38]	DDoS	Gas limits, Legacy IoT devices	Ethereum	Smart contracts	Ethereum limitations
Al-Shakran *et al.* [39]	DDoS	Botnet prevention, Blacklisting IPs	Unspecified	SDN, Smart contracts	SDN risks
Asiri and Miri [41]	Sybil	Trust among IoT devices	Hyperledger Fabric	None	Limited trust criteria
Rechained [43]	Sybil	Access control, Tokenisation	Bitcoin	None	Bitcoin limitations

7 Discussion

Many of the proposed IoT security frameworks provide a high-level architecture as a solution to either DDoS attacks or Sybil attacks. In some cases this solution is then implemented on a PC and tested with simulations. Notwithstanding a quantitative first approach in testing the framework, this does not resemble large scale IoT infrastructures on which the frameworks need to be deployed. Moreover, most papers do not describe a testing approach and merely explain their framework and give an architectural overview. For researchers comparing these frameworks, quantification of tests in any form is more forthright. Hence, other researchers of blockchain-based IoT security frameworks are encouraged to run the implementations on constrained devices or to run simulations, showing results of their frameworks. Comprehensive results in terms of network performance, cost, energy efficiency and scalability will make the comparison of different frameworks conveniently quantifiable for comparative studies.

To conclude this section, there are many security risks as a result of the many cyber attacks possible in the IoT as portrayed by [10] and [9]. This research only focused on proposed blockchain-based solutions specifically for mitigating DDoS attacks and Sybil attacks to try and start filling the gap in literature with regards to blockchain-based IoT security. Other researchers are suggested to highlight other attacks within the IoT and compare different solutions and frameworks, both blockchain-based and alternatives such as DAG approaches as can be found in [49], [50], [51] and [52].

8 Responsible Research

This section will reflect on the ethical aspects of the research and the reproducibility of the research methods and approach.

8.1 Ethics of blockchain technology within the IoT

This paper is a literature study in which several blockchain-based frameworks are highlighted and compared with each other. There are no direct ethical aspects in terms of user testing and participation, as this research is literature-based without human research subjects. However, the nature of the contents and topics can have various positive and negative ethical aspects within society.

Many ethical aspects arise when security is at stake in the IoT. IoT devices collect and share massive amounts of data that could be private and confidential, as can be seen in industries such as healthcare or even defence. The effects of possible cyber attacks as a result of current IoT security issues can be tremendous as is seen in previous examples of real-life attacks [20]. Solving these issues has thus positive ethical implications for society. However, the use of blockchain specifically in solving these problems can have negative societal aspects as well [53].

Because of its improved security aspects compared to centralised models, blockchain relies on consensus mechanisms that can be computationally heavy and thus requiring incredible amounts of electricity [54]. This resource-intensive design of blockchain implementations such as Bitcoin's Proof of Work, pose a serious threat to the global commitment to mitigate greenhouse gas emissions [55], [53]. As a result of this, various policies are currently being researched and proposed in order to limit the environmental impact of the use of blockchain technology [55]. Furthermore, in the blockchain-based IoT domain, many alternative consensus mechanisms are researched and compared, requiring less resources and having a smaller impact on the environment [53], [56].

8.2 Reproducible research

Several blockchain-based frameworks are highlighted and compared in this research paper. These frameworks are compared based on the technologies used and the security goals expected to be achieved, as described in the papers of the authors. Because most of these papers did not provide quantitative test results, thus comparing them on features such as network performance and cost was not possible. A table is made to summarise the comparison of the frameworks, highlighting the most important features and limitations. The reasoning behind the comparison results and information regarding potential drawbacks of mentioned frameworks is explained and based on existing literature that is provided in the References section, making this research reproducible.

9 Conclusions and Future Work

The IoT is an emerging movement within the technology world that promises growth and ease for humans in many industries such as healthcare and smart cities. However, current IoT infrastructures are heavily centralised and face challenges in terms of security, privacy and trust. Proposed blockchain solutions show promising results in securing the IoT. Although blockchain has its own drawbacks such as computational complexity and energy usage, research still needs to look into scalable and more green solutions to provide security of the ever-growing IoT domain. This research has focused on blockchain-based solutions for mitigating DDoS attacks and Sybil attacks in the IoT. Quantification of result data is most of the time not present, making the comparison of different framework solutions complicated and qualitative in nature. Researchers looking into blockchain-based IoT frameworks are advised to provide quantifiable test results, this makes comparison studies more accessible for other researchers in the field. For future research, it is advised to look into other security attacks and compare specific blockchain-based solutions for them. Alternative solutions for various security risks can also be looked in to, such as the DAG approaches. Finally, there are other aspects and issues of the IoT such as privacy and trust. Combining frameworks and proposing blockchain-based solutions that touch these aspects in combination with security is a logical next step in future research.

References

[1] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim, “An in-depth analysis of the mirai botnet,” in *2017 International Conference on Software Security and Assurance (ICSSA)*, 2017, pp. 6–12.

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the mirai botnet,” in *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[3] G. Kambourakis, C. Kolias, and A. Stavrou, *The Mirai botnet and the IoT Zombie Armies*, 2017.

[4] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, “Iot security: Ongoing challenges and research opportunities,” in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, 2014, pp. 230–234.

[5] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of blockchains in the internet of things: A comprehensive survey,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[6] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, “Internet of things (iot) security: Current status, challenges and prospective measures,” in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015, pp. 336–341.

[7] L. Da Xu, Y. Lu, and L. Li, “Embedding blockchain technology into iot for security: A survey,” *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[8] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, “A survey on the integration of blockchain with iot to enhance performance and eliminate challenges,” *IEEE Access*, vol. 9, pp. 54 478–54 497, 2021.

[9] S. Singh, A. S. M. S. Hosen, and B. Yoon, “Blockchain security attacks, challenges, and solutions for the future distributed iot network,” *IEEE Access*, vol. 9, pp. 13 938–13 959, 2021.

[10] J. Sengupta, S. Ruj, and S. Das Bit, “A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot,” *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519303418

[11] A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for iot,” in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2017, pp. 173–178.

[12] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[13] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, “Analysis of ddos-capable iot malwares,” in *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2017, pp. 807–816.

[14] N. Vlajic and D. Zhou, “Iot as a land of opportunity for ddos hackers,” *Computer*, vol. 51, no. 7, pp. 26–34, 2018.

[15] N. Kshetri, “Can blockchain strengthen the internet of things?” *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[16] M. A. Khan and K. Salah, “Iot security: Review, blockchain solutions, and open challenges,” *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17315765

[17] D. Minoli and B. Occhiogrosso, “Blockchain mechanisms for iot security,” *Internet of Things*, vol. 1-2, pp. 1–13, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660518300167

[18] R. Minerva, A. Biru and D. Rotondi, "Towards a definition of the internet of things," *IEEE Internet Initiative*, vol. 1, pp. 1–86, 2015.

[19] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[20] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[21] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, p. 1645–1660, 2013. [Online]. Available: https://dx.doi.org/10.1016/j.future.2013.01.010

[22] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.

[23] S. Shapsough, F. Aloul, and I. A. Zualkernan, "Securing low-resource edge devices for iot systems," in *2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI)*, 2018, pp. 1–4.

[24] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[25] M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency," *Annals of Emerging Technologies in Computing*, vol. 2, no. 1, p. 1–6, Jan 2018. [Online]. Available: http://dx.doi.org/10.33166/AETiC.2018.01.001

[26] G. Karame and S. Capkun, "Blockchain security and privacy," *IEEE Security Privacy*, vol. 16, no. 04, pp. 11–12, jul 2018.

[27] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 27–51, 2015.

[28] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[29] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn security: A survey," in *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, 2013, pp. 1–7.

[30] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[31] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," Oct 2018. [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.8202

[32] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied Sciences*, vol. 9, no. 9, 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/9/1788

[33] C. Ye, G. Li, H. Cai, Y. Gu, and A. Fukuda, "Analysis of security in blockchain: Case study in 51International Conference on Dependable Systems and Their Applications (DSA), 2018, pp. 15–24.

[34] A. Lohachab and B. Karambir, "Critical analysis of ddos—an emerging security threat over iot networks," *Journal of Communications and Information Networks*, vol. 3, no. 3, p. 57–78, 2018.

[35] Z. A. El Houda, A. Hafid, and L. Khoukhi, "Co-iot: A collaborative ddos mitigation scheme in iot environment based on blockchain using sdn," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[36] N. Giri, R. Jaisinghani, R. Kriplani, T. Ramrakhyani, and V. Bhatia, "Distributed denial of service(ddos) mitigation in software defined network using blockchain," in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2019, pp. 673–678.

[37] Q. Shafi and A. Basit, "Ddos botnet prevention using blockchain in software defined internet of things," in *2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2019, pp. 624–628.

[38] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating lot device based ddos attacks using blockchain," ser. CryBlock'18. New York, NY, USA: Association for Computing Machinery, 2018, p. 71–76. [Online]. Available: https://doi.org/10.1145/3211933.3211946

[39] H. Al-Sakran, Y. Alharbi, and I. Serguievskaia, "Framework architecture for securing iot using blockchain, smart contract and software defined network technologies," in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, 2019, pp. 1–6.

[40] H. Sato, A. Kanai, S. Tanimoto, and T. Kobayashi, *Establishing Trust in the Emerging Era of IoT*, 2016.

[41] S. Asiri and A. Miri, "A sybil resistant iot trust model using blockchains," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1017–1026.

[42] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[43] A. Bochem and B. Leiding, "Rechained: Sybil-resistant distributed identities for the internet of things and mobile ad hoc networks," *Sensors*, vol. 21, no. 9, p. 3257, 2021.

[44] K.-C. Yen and H.-P. Cheng, "Economic policy uncertainty and cryptocurrency volatility," *Finance Research Letters*, vol. 38, p. 101428, 2021.

[45] D. Kreutz, F. M. Ramos, and P. Verissimo, *Towards secure and dependable software-defined networks*, 2013.

[46] M. Valenta and P. Sandner, "Comparison of ethereum, hyperledger fabric and corda," *Frankfurt School Blockchain Center*, vol. 8, 2017.

[47] H. Liu, D. Han, and D. Li, "Fabric-iot: A blockchain-based access control system in iot," *IEEE Access*, vol. 8, pp. 18 207–18 218, 2020.

[48] D. Vujicic, D. Jagodic, and S. Randic, *Blockchain technology, bitcoin, and Ethereum: A brief overview*, 2018.

[49] A. Cullen, P. Ferraro, C. King, and R. Shorten, "On the resilience of dag-based distributed ledgers in iot applications," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7112–7122, 2020.

[50] L. Zhao and J. Yu, "Evaluating dag-based blockchains for iot," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2019, pp. 507–513.

[51] C. Fan, H. Khazaei, Y. Chen, and P. Musilek, "Towards a scalable dag-based distributed ledger for smart communities," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, pp. 177–182.

[52] B. Shabandri and P. Maheshwari, "Enhancing iot security and privacy using distributed ledgers with iota and the tangle," in *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, 2019, pp. 1069–1075.

[53] C. Schinckus, "The good, the bad and the ugly: An overview of the sustainability of blockchain technology," *Energy Research Social Science*, vol. 69, 2020.

[54] P. Giungato, R. Rana, A. Tarabella, and C. Tricase, "Current trends in sustainability of bitcoins and related blockchain technology," *Sustainability*, vol. 9, no. 12, p. 2214, 2017. [Online]. Available: https://dx.doi.org/10.3390/su9122214

[55] J. Truby, "Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies," *Energy Research Social Science*, vol. 44, p. 399–410, 2018.

[56] Y. Wen, F. Lu, Y. Liu, P. Cong, and X. Huang, *Blockchain Consensus Mechanisms and Their Applications in IoT: A Literature Survey*. Transactions on Large-Scale Data- and Knowledge-Centered Systems XLVIII, 2020, p. 564–579.