International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 09
August 2019

A Survey on DDoS Mitigation Using Blockchain

Saee M. Joshi
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
saee.joshi46@gmail.com

Prof. Dr. K. Rajeswari
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
kannan.rajeswari@pccoepune.org

Abstract— **Blockchain is a digital tracker that maintains instant and permanent records validated across a specific chain of computers. This process makes it easy to spot fraudulent behavior, making the transaction more secure. Hence it is very much important to ex plore on such emerging technologies which will be essential for applications such as Smart Property, Smart Contracts, Internet of Things, Financial Services etc. Attacks like Distributed Denial-of-Service (DDoS) pose a growing threat to computer networks and internet services. Existing strategies for mitigating DDoS attacks are inecient because of lacking resources and inexibility. Blockchains like Ethereum enable new ways to prevent against DDoS attacks: Using smart contracts, IP addresses of attackers can be signalized without additional infrastructure. The exponential increase of traffic volume makes DDoS attacks a top security threat to service providers and addressing this is the crux of Blockchain Technology. Bitcoin has been the most popular cryptographic currency since it was invented and it is the best example that uses the Blockchain technology. To avoid an attack, the network uses the Blockchain consensus which addresses various algorithms such as Proof-of-Work(PoW), Proof-of-Stake(PoS) etc. This seminar work focuses on studying how Blockchain can be used as a Security Mechanism to prevent Ddos Attacks which may also provide insights for implementation of certain applications.**

I. INTRODUCTION

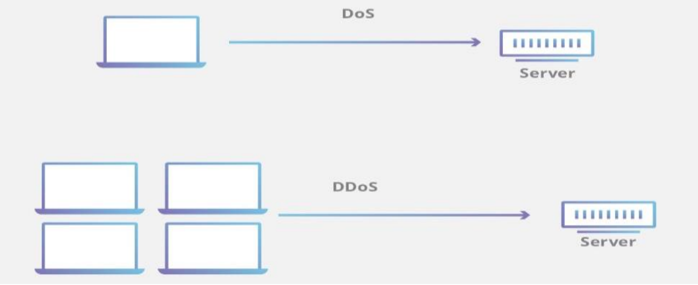
A. DDoS

A Distributed Denial of Service (DDoS) attack is a DoS attack where the requests are coming from many different sources. By distributing the requests, a Denial of Service attack can reach much higher magnitudes in terms of traffic and can become much harder to control. Usually, an attacker takes control of as many internet-connected devices as possible by spreading malware, and then directing these devices to attack the victim [4]. A DDoS attack can be stopped by blocking the traffic from the attacker. Each traffic package contains information about the source, including an identifier called the IP(Internet Protocol) address. By filtering the traffic based on the source IP address, the attack can be mitigated [4].

Victims of DDoS attacks can receive help by identifying the source IP addresses of attackers and notifying the upstream providers, so that they can block traffic before it reaches the victims infrastructure [4]. DDoS attacks have a simple goal of interrupting or suspending internet services for various motivations ranging from personal interests, business tricks etc. A very large DDoS attack was detected in the GITHUB website very recently. Besides frequency the strength and the duration of the attack is also growing rapidly making DDoS attacks more effective. An infrastructure of blockchains and smart contracts will provide the required mechanism without the need to maintain development complexities of such a new protocol. The development of a DDoS attack is mainly dependent on the number of BOTS. By exploting legal srvices on the device the power of a DDoS attack is amplified[1].

A blockchain is a decentralized database consisting of crytographically secured units called blocks. A blockchain keeps growing as data is entered at the end of the chain. The most widely implemented blockchain is Bitcoin. The most popular application for blockchains is crypto currencies. With blockchain technology each page in a ledger of transaction forms a block [3]. That block has an impact on the next block or page trough cryptographic hashing.In other words,when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or blockchain. The most remarkable feature about blockchain is that it increase the capacity of the whole network. Even in the highest level financial systems are getting hacked. Bitcoin on the other hand has never been hacked. Blockchain technology has a better security because there is not even a single chance of shutting down of the system [6].

Fig. 1. DoS and DDoS



B. Blockchain and Smart Contracts

The advantage of using smart contracts in a blockchain is :

(a) To make use of an already existing infrastructure to distribute rules without the need to build specialized registries or other distribution mechanisms/protocols.
(b) To apply rules across multiple domains, which means that even if the AS (Autonomous System) of the victim is not applying these rules, some traffic can still be filtered.

(c) The victim or its AS can control which customers get blocked. The only central element remaining is to show proof of IP ownership [2].

Software-defined Network (SDN) is an effective solution to enable customizable security policies and services in a dynamic fashion. The centralized network control and its deployment based on the OpenFlow protocol facilitates the enforcement of high-level security policies moving away from current approaches based on SNMP (Simple Network Management Protocol) and CLI (Command Line Interface)[5]. With SDN, flowrules can be applied to block DDoS attacks, and the closer these rules are applied, and those malicious packets can be dropped, the less DDoS traffic occurs [9]. This work uses SDN-based networks as a use case to perform in a more rapid fashion in ASes the definition and verification of flows to mitigate DDoS attacks. However, the presented solution is not limited to the usage of an SDN-based network, being compatible with detection/monitoring tools able to export attack information to be published in blockchain [2].

C. *Ethereum*

Ethereum : Ethereum is a blockchain protocol inspired from Bitcoin, but not only allows for sending and receiving of tokens, but also offers a scripting language called solidty which allows anyone to write programs which can run on blockchains. Games like Tic-Tac-Toe or Poker are applications that run on Ethereum. Ethereum provides a decentralized Turing complete virtual machine known as the Ethereum Virtual Machine (EVM).It is used for executing scripts using an international network of public nodes. Ether can be transferred between accounts and used to compensate participation mining nodes for computations performed. Ethereum is open sourced [6].

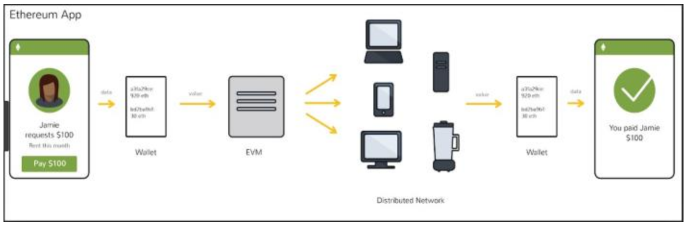


Fig. 2. Working of Ethereum

D. *Smart Contracts*

Smart contracts are contracts that help any form of transaction without the interference of third party users. Ethereum smart contracts allows for storage of binary information. They help in transactions that mutate the storage. By writing the code, the smart contract creator can control permissions of the users and the conditions and behaviour of the mutations [6].

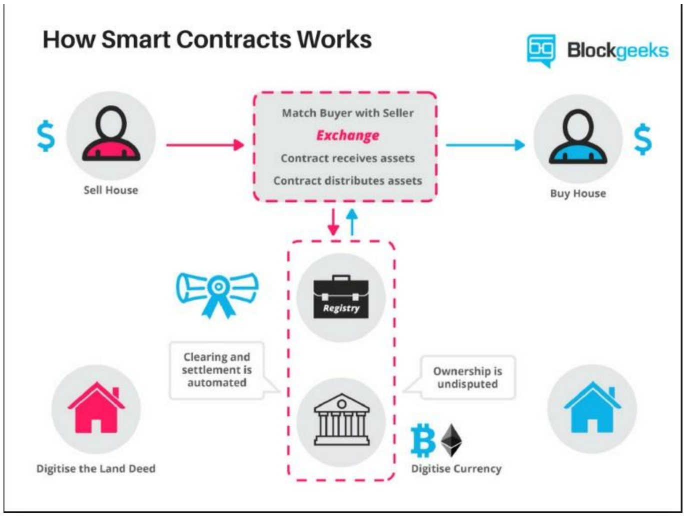


Fig. 3. Working of an Smart Contract

II. LITERATURE SURVEY

- **”Muti-Domain DDoS Mitigation based on Blockchain”, Bruno Rodriguous , Thomas Bocek , Burkhard Stiller , Springer, 2019**

  This article [1], says that the exponential increase of the traffic volume makes DDoS attacks a top security threat to service providers. Existing DDoS defence mechanism lack resources and flexibility to cope with attacks by themselves, and buy other companies resources the burden of mitigation can be shared.Technologies like Blockchain and Smart Contracts allow distributing attack information across multiple domains, while SDN(Software-Defined Networks) and NFV(Network Function Virtualization) enables to scale defence capabilities on dmand for single network domain. Blockchain and Smart Contracts are introducing novel opportunities for flexible and efficient DDoS mitigation solutions across multiple domains.

- **”A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts”, Bruno Rodrigues, Thomas Bocek, Andri Lareida, David Hausheer, Sina Rafati, and Burkhard Stiller, University of Zurich (UZH), Switzerland, 2017**

This paper[2], says that the rapid growth in the number of insecure portable and stationary devices and the exponential increase of traffic volume makes Distributed Denial-of-Service (DDoS) attacks a top security threat to services provisioning. Existing defense mechanisms lack resources and flexibility to cope with attacks by themselves, and by utilizing others companies resources, the burden of the mitigation can be shared. Emerging technologies such as blockchain and smart contracts allows for the sharing of attack information in a fully distributed and automated fashion. In this paper, the design of a novel architecture is proposed by combining these technologies introducing new opportunities for flexible and efficient DDoS mitigation solutions across multiple domains. Main advantages are the deployment of an already existing public and distributed infrastructure to advertise white or blacklisted IP addresses, and the usage of such infrastructure as an additional security mechanism to existing DDoS defense systems, without the need to build specialized registries or other distribution mechanisms, which enables the enforcement of rules across multiple domains.

- **”Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Signaling System (BloSS)” , Bruno Rodrigues, Thomas Bocek, Burkhard Stiller, University of Zurich (UZH), 2017**

This paper [3], describes that Distributed Denial- of-Service (DDoS) defense systems are not capable of withstanding by themselves against large-scale attacks. Thus, coordinated protection efforts have become an attractive alternative to extend defense capabilities of a single system. However, existing DDoS signaling protocols are a bottleneck to make a coordinated and distributed defense fully operational. Blockchain technology offers an out-of-the-box solution that not only reduces the complexity of signaling DDoS attack information, but could also provide means of establishing financial incentives, for cooperation at a reduced operational cost. This work presents the Blockchain Signaling System (BloSS), a novel approach deploying hardware to simplify the signaling of DDoS attacks in a cooperative network defense system.

- **”Collaborative DDoS Mitigation Based on Blockchains”, Bruno Rodrigues, Thomas Bocek, Burkhard Stiller, University of Zurich (UZH), 2017**

This paper[4], describes that attacks like Distributed Denial-of-Service (DDoS) pose a growing threat to computer networks and internet services. Existing strategies for mitigating DDoS attacks are inefficient because of lacking resources and inflexibility. Blockchains like Ethereum enable new ways to fight DDoS attacks: Using smart contracts, IP addresses of attackers can be singalized without additional infrastructure. This work documents the development of multiple smart contracts for signalisation of DDoS attacks and compares them, describes the Ethereum environment and its effect on the smart contract architecture, gives information and advice about the performance and costs and evaluates the overall feasability and effectivity of a blockchain-based solution for fighting DDoS attacks.

- **”CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourcing”, Ming Li, Jian Weng, Anjia Yang, Wei Lu,Yue Zhang, Lin Hou, Jia-Nan Liu, Yang Xiang, Robert H. Deng, IEEE 2018**

This paper[5], says that crowdsourcing systems which utilize the human intelligence to solve complex tasks have gained considerable interest and adoption in recent years. However, the majority of existing crowdsourcing systems rely on central servers, which are subject to the weaknesses of traditional trust-based model, such as single point of failure. They are also vulnerable to distributed denial of service (DDoS) and Sybil attacks due to malicious users involvement. In addition, high service fees from the crowdsourcing platform may hinder the development of crowdsourcing. How to address these potential issues has both research and substantial value. In this paper, we conceptualize a blockchain-based decentralized framework for crowdsourcing named CrowdBC, in which a requesters task can be solved by a crowd of workers without relying on any third trusted institution, users privacy can be guaranteed and only low transaction fees are required. In particular, we introduce the architecture of our proposed framework, based on which we give a concrete scheme. We further implement a software prototype on Ethereum public test network with real-world dataset. Experiment results show the feasibility, usability and scalability of our proposed crowdsourcing system.

- **”DDoS Mitigation Using Blockchain”, J. Dheeraj, S. Gurubharan, International Journal of Research in Engineering, Science and Management(IJRESM), 2018**

This paper[6], says that the rapid growth in the number of insecure portable and stationary devices and a large increase in Internet traffic makes Distributed- Denial- of -Service a top security threat. Existing defensive mechanism lack resources and flexibility

to cope with the attacks themselves. Emerging technologies like block chain and smart contracts can be used for the mitigation of DDoS attacks as it allows for the sharing of attack information in a fully distributed and automated fashion. In this paper, an architecture is designed combining these technologies introducing new opportunities for an effective DDoS mitigation. This paper presents the architecture and design of a collaborative mechanism using blockchains and smart contracts. The objective is to create an automated and easy to manage mechanism for DDoS mitigation.

III. SYSTEM ARCHITECTURE

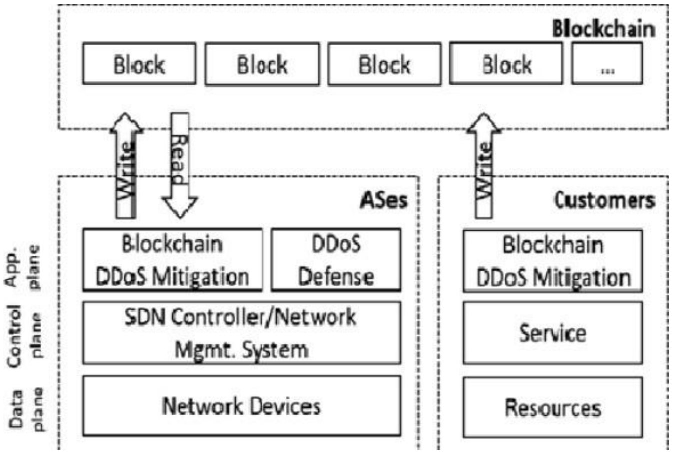


Fig. 4. System Architecture [6]

To mitigate DDoS attacks different techniques can be used which involves analyzing internet traffic using diiferent algorithms for attack detection and filtering them. The collaborative approach decreases the necessity of such algorithms in the detection phase using information from other domains. Any domain participating must create a smart contracts identified with the IP addresses and the range of IP addresses certified by an authority. Then the smart contract is registered so that participation can easily be tracked and thus relevant smart contracts can be identified.

IV. BLOCKCHAIN AS A SOLUTION

The use of Ethereum Virtual machine allows for multiple domains involved in an attack scenario to invoke functions in smart contracts which reports attacks or maintains a list of trusted IP addresses to be operating in case of an attack. The support of blacklist or whitelist IP addresses is the decision that depends on the security policies of the particular domain [7]. Therefore smart contracts have been developed in such a way to support both types of lists using a flag indicating which type of address it is. The existing and distributed storage infrastructure reduces the complexity in the development of the approach as it supersedes the design

and standardization process of a gossip- based protocol. Also, the EVM smart contracts support in a decentralized and native way the logic to control who is reporting the attack and who are the attacker.

Through a high level comparison with the ongoing IETF proposal, instead of making use of an existing infrastructure such as blockchain and smart contracts, IETF proposes the development of such protocol with several requirements to be deployed in a distributed architecture [8]. In this sense the protocol development becomes complex since it must be deployed in a centralized architecture to support different types of communication. Instead it can be argued that some of the requirements can be inherited from the characteristics of the blockchains and smart contracts. This avoids complexity in the development and adoption of new protocols.

However, this smart contracts works well only for a small number of attacks, while for a large number of attacks the approach is rather costly. Therefore to keep the complexity of the architecture low only the data of the IP address must be stored in the smart contracts. The cost of adding 50 source IP address in a freshly deployed smart contract is 9.3 USD, while 100 IP addresses cannot be stored in one contract.

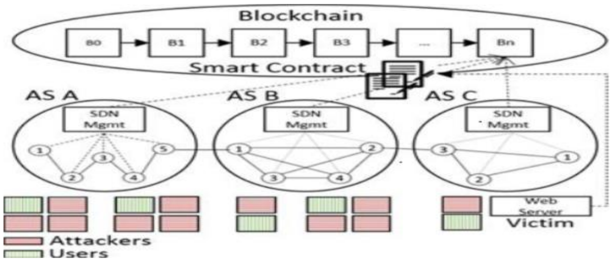


Fig. 5. Application Scenario [6]

V. CONCLUSION

A collaborative architecture using smart contracts is used to enable DDoS mitigation across multiple domains. As a distributed and primarily public storage, the blockchain determines a straightforward and efficient structure to develop a collaborative approach towards DDoS attack mitigation. The proposed architecture can be considered as an additional security to already existing techniques.

It can be combined with existing solutions to reduce the DDoS attacks. Coupled with current solutions, the DDoS detection and mitigation overhead process comprising multiple domains can be reduced. The architecture enables ASes to deploy their DPS(Damage Per Second) and generate added value for their customers without transferring control to their network to a third party.

REFERENCES

[1] Muti-Domain DDoS Mitigation based on Blockchain , Bruno Rodriguous ,Thomas Bocek , Burkhard Stiller , Springer, 2019.

[2] A Blockchain-Based Architecture for Collaborative DDoS Mitigation withSmart Contracts, Bruno Rodrigues, Thomas Bocek, Andri Lareida, DavidHausheer, Sina Rafati, and Burkhard Stiller, University of Zurich (UZH), Switzerland, 2017.

[3] Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Sig-naling System (BloSS) , Bruno Rodrigues, Thomas Bocek, Burkhard Stiller,University of Zurich (UZH), 2017.

[4] Collaborative DDoS Mitigation Based on Blockchains, Bruno Rodrigues,Thomas Bocek, Burkhard Stiller, University of Zurich (UZH), 2017.

[5] CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourc-ing, Ming Li, Jian Weng, Anjia Yang, Wei Lu,Yue Zhang, Lin Hou, Jia-NanLiu, Yang Xiang, Robert H. Deng, IEEE, 2018.

[6] DDoS Mitigation Using Blockchain, J. Dheeraj, S. Gurubharan, Interna-tional Journal of Research in Engineering, Science and Management (IJRESM), 2018.

[7] Comparative Analysis of Blockchain Consensus Algorithms, L.M. Bach , B. Mihaljevic and M. Zagar , MIPRO, 2018.

[8] A Review on Consensus Algorithm of Blockchain, Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun, IEEE, 2017.

[9] Prevention of DDoS attacks with Blockchain technology, Deloitte, 2017.