DoS Attacks on Blockchain Ecosystem

Mayank Raikwar[0000−0002−5479−5748] and Danilo Gligoroski[0000−0002−7078−6139]

Norwegian University of Science and Technology (NTNU) Trondheim, Norway
{mayank.raikwar,danilog}@ntnu.no

Abstract. Denial of Service (DoS) attacks are a growing threat in network services. The frequency and intensity of DoS attacks are rapidly increasing day by day. The immense financial potential of the Cryptocurrency market is a prevalent target of the DoS attack. The DoS attack events are kept on happening in cryptocurrencies and the blockchain ecosystem. To the best of our knowledge, there has not been any study on the DoS attack on the blockchain ecosystem. In this paper, we identify ten entities in the blockchain ecosystem and we scrutinize the DoS attacks on them. We also present the DoS mitigation techniques applicable to the blockchain services. Additionally, we propose a DoS mitigation technique by the use of verifiable delay function (VDF).

Keywords: Denial-of-service · Verifiable Delay Function· Non-Interactive · Blockchain

1 Introduction

Blockchain had brought a paradigm shift in digital innovation and the financial world since the advent of Bitcoin [26]. Today, the cryptocurrency market consists of 5424 cryptocurrencies that all together built a financial market worth around $1.71 trillion (as of 26 May 2021) [9]. The immense financial potential of the cryptocurrency market has become a growing concern for the targeted attacks. Some of the well-known attacks in current blockchain systems are selfish mining, blockchain forks, 51% attack, double spending, Sybil attack, and Denial-of-service attacks [33]. A Denial-of-service (DoS) attack prevents legitimate user requests and depletes the server's resources. Due to the various configurations and decentralized features of blockchain, many of the attacks are preventable. Nevertheless, DoS attacks, especially its distributed variant (DDoS), are still prominent attacks on cryptocurrencies and blockchain-based applications.

Due to the increasing intensity and frequency of DoS attacks, it is contemplated as one of the biggest and severe threats for the Internet industries. One of the major DoS attacks was mounted on a DNS server in October 2016, which manifested in a cut of access to major websites, including PayPal, Netflix, and Twitter, for several hours [46]. The spectrum of DoS attacks can range from DNS services, cloud providers, IoT devices to the cryptocurrency and blockchain market. Nowadays, the cryptocurrency market is a popular target of DoS attacks, with the motivation of ransom, stealing funds, or business competition. In the

past, many works[21,19,12] regarding the detection and prevention of DoS attacks have been carried out. Moreover, DoS/DDoS solutions based on blockchain are an emerging area of research. Applying the most recent advances of cryptographic research for the DoS/DDoS[1] problem can open new directions and avenues for addressing this ever-present problem.

In the general context of a DoS attack in blockchain, an adversary usually mounts a DoS attack when the cost of mounting an attack is very low. Therefore, various countermeasures, such as increased block size, increased transaction fees, or limiting transaction size have been proposed for mitigating the attacks. However, most of these countermeasures also force legitimate system users to invest their economic or computational power. This behavior shows a dire need to construct new methods for DoS prevention that do not require extra-economic or computational power of blockchain users. In this paper, we study and review DoS attacks on ten different entities in the blockchain ecosystem and possible mitigation techniques. In addition, we propose DoS mitigation by applying the astonishing functionality of verifiable random function (VDF) [8].

1.1 Related Work

Many DoS attacks have been mounted in the blockchain ecosystem and its services in the past few years. Some of these DoS attacks or threats on cryptocurrencies were disclosed a couple of years after they had been discovered. It requires new techniques to detect and counter the attack. Some of those new blockchain-based DoS mitigation techniques are devised from the decentralized nature and the deployed smart contracts of blockchain [30,36]. Even different machine learning techniques have been proposed to fight the DoS attack in cryptocurrency [14].

Specifically for the Bitcoin blockchain (as the blockchain of the most popular and valuable cryptocurrency), several DoS attacks have been mounted [40], which include mining pools, currency exchanges, eWallets, and financial services. Like most high visibility businesses, mining pools and currency exchanges are the primary DoS targets, which drives them to buy DDoS protection services such as Incapsula, CloudFlare, or Amazon Cloud. A report from September 2020 [18] revealed that the Bitcoin software implementation had a vulnerability for an uncontrolled memory consumption that was repeatedly used as a DoS vulnerability until it was patched in June 2018. This DoS vulnerability existed in many other branched Bitcoin implementations, including Litecoin and Namecoin.

Another major cryptocurrency, Ethereum [45] has also suffered from DoS attack [4]. In September 2016, a DoS attack against the Ethereum network was begun by exploiting a flaw in its client node. Furthermore, the same week, another DoS attack was mounted on the processing nodes of Ethereum [44]. A recent disclosure on Ethereum shows that a very cheap DoS attack could have brought down the Ethereum main net due to a bug in Geth Ethereum client [16].

[1] Throughout the paper, we use DoS to refer to both DoS and DDoS attacks, unless explicitly mentioned.

Recent work shows an Incentive-based blockchain denial of service attack (BDoS) [25] on Proof-of-work-based blockchains that exploits the reward mechanism to discourage the miner participation. This BDoS could theoretically be able to grind the (Bitcoin's) blockchain to a halt with significantly fewer resources (21% of the network's mining power). This attack raises a concern about the liveness of the Proof-of-work-based cryptocurrencies. This big concern and recent ongoing DoS attack disclosures compel researchers to find new ways to construct efficient DoS mitigation techniques.

1.2 Denial of Service Attack

A denial of service (DoS) attack targets to disrupt the availability of the network, server or application, and prevents legitimate requests from taking place. For a DoS attack to be successful, the attacker has to send more requests than the victim server can handle. These requests can be legitimate or bogus. The DoS attack depletes the server's resources such as CPU, memory, or network.

Definition 1. *(DoS): Let a server $\mathcal{S}$ be given, with the available resources $R_1, R_2, \ldots, R_n$ (R_i can be bandwidth, memory, CPU etc.). Let $\mathcal{A}$ or a set of $\{\mathcal{A}_j\}$ are an attacker or a set of attackers and let the legitimate users are represented by the set $\{\mathcal{U}_k\}$. A DoS attack on server $\mathcal{S}$ is expressed by a set of probabilities for successful resource-depletion $\{P_{R_1}, P_{R_2}, \ldots, P_{R_n}\}$. The total probability for a success of a DoS attack is then a probability the server $\mathcal{S}$ to refuse legitimate transactions from a user u, where $u \in \{\mathcal{U}_k\}$ and is modeled as the probability of blocking the legitimate traffic in at least one of the resources:*

$$P_{DoS} = 1 - (1 - P_{R_1})(1 - P_{R_2}).\ldots.(1 - P_{R_n}) \tag{1}$$

Note that the situation when attacker(s) exhausts at least one resource R_i implies the attack probability is $P_{R_i} = 1$, which from equation (1) further leads to $P_{DoS} = 1$.

DoS attacks can be categorized into several categories based on network and application layers or volume and protocol attacks. Network-level DoS attacks aim to overload the server's bandwidth or cause CPU usage issues. However, application-level DoS attacks focus on applications, websites, or online services.

1.3 Our Contribution

The contributions of our work are as follows:

1. We thoroughly investigate the DoS attacks in the blockchain ecosystem.
2. We present different mitigation techniques of DoS attacks in the blockchain ecosystem.
3. We propose a VDF-based DoS resistant protocol by using the functionality of VDF.

The rest of the paper is as follows: Section 2 shows a detailed analysis of DoS attacks in the blockchain ecosystem. Further, Section 3 presents DoS mitigation techniques, including our VDF-based proposal. Finally, in Section 4, we conclude the paper and discuss the possible future directions.

2 DoS Attacks on Blockchain Ecosystem

The blockchain ecosystem has suffered from many DoS attacks in the past, and that situation is a continuing trend. The DoS attack can be launched against a specific entity or a network in the blockchain. We present a nonexclusive list of ten entities in the Blockchain ecosystem with their corresponding DoS attacks.

1. *On cryptocurrency wallets* A crypto wallet is a software program in which a user stores cryptocurrency. The wallet contains a set of signing keys for the user to sign new transactions. Wallets are also integrated with decentralized applications (DApps) to hold and manage users' signing keys and transactions securely. In a wallet service, a user is the sole owner of his account keys. However, if someone steals the signing keys, then the cryptocurrency held in that account can be spent. Therefore, hardware wallets (e.g., TREZOR) are ways to store cryptocurrency and the signing key in an offline manner. Nevertheless, online wallets are still a preferable choice for blockchain users. These online crypto wallets also suffer from DoS attacks [28] due to inconsistency in its smart contracts that further hinders the services of integrated DApps. Recently, a DDoS attack was mounted on the Wasabi bitcoin wallet [15].
2. *On cryptocurrency exchange services* A cryptocurrency exchange allows clients to buy, sell and store crypto-currencies at some exchange rate and leverages the clients to trade their currencies and earn some profit due to the fluctuations in the price of currencies. Besides, the exchange charges some fee for every trade made by its client and also converts the cryptocurrency into fiat currencies. Many exchange services also provide a wallet, but the wallet signing keys are controlled by the exchange service apart from the wallet user. Furthermore, these exchange services are online platforms, hence susceptible to DoS attacks that can cause the temporary unavailability of the platform. In the past, many of the crypto-currency exchange services were jeopardized by the DoS attacks (especially DDoS). One such example is the Bitcoin exchange platform, *Bitfinex* which has been a victim of DDoS attacks several times [2]. Another well-known bitcoin exchange service, Mt. Gox, was completely disrupted by DDoS attacks over time [17]. Over the years, many cryptocurrency exchange platforms have suffered DoS attacks. Recently, a UK-based exchange *EXMO* was hit by DDoS attack [10].
3. *On memory (transaction) pools* A memory pool (mempool) is a repository of unconfirmed transactions in a cryptocurrency blockchain, e.g., Bitcoin. Once a user creates a new transaction, it is broadcast to the network and stored in the mempool. In the mempool, the transaction waits to be picked by a miner to be added in a block and subsequently to the blockchain, therefore acquiring the transaction's confirmation. If a transaction remains unconfirmed for a long time in the mempool, it gets rejected eventually. As the transactions with high fees are most likely to be selected by a miner, it poses a threat to flood the mempool by small fee transactions, consequently affecting the mempool size. In that direction, it creates uncertainty among the users for their transactions and leads them to pay higher mining fees to prevent the

rejection of their transactions. The work [34] studies such an attack on Bitcoin mempool and proposes a few countermeasures. However, the proposed solutions have limitations regarding the minimum payable fee and rejection of fast transactions. A follow-up work [32] provides similar prevention measures for Proof-of-work-based blockchain but suffers from the similar problems.

4. *On mining pools* Mining pools are the major players in Proof-of-work-based cryptocurrencies, e.g., Bitcoin. The mining pool's goal is to accumulate miners' power and solve the Proof-of-work puzzles. As the difficulty of Proof-of-work puzzles gives a very low probability of solving the puzzle to a single miner, the miner usually prefers to join a mining pool where the miner gets a fair share of the reward proportional to his/her effort, if the mining pool finds the solution. Two kinds of entities can mount a DDoS attack on a mining pool: 1) A hacker whose aim is to make money by asking the ransom from the attacked mining pool with the promise of stopping the DDoS attack [22], 2) A competing mining pool whose goal is to increase his winning probability by undermining the power of competing mining pools. Few game-theoretic studies [48,47] are also conducted to analyze DoS attacks in mining pools.
5. *On layer-two blockchain protocols* Layer-two blockchain protocols are built on the top of the main blockchain that moves a sufficient amount of transaction load from the main blockchain to the off-chain in sub-seconds (instead of minutes or hours) with a reduced fee and similar security. Hence, these protocols are referred to as an orthogonal solution for the scalability problem in the blockchain. In recent years, there has been tremendous growth in constructing new layer-two protocols [20] for blockchain scalability such as channel networks. In a channel network, channels are established between the parties of the network and governed by the smart contracts of the main chain. It provides a fast and scalable approach for off-chain interactions. These protocols also suffered from DoS attacks in the past [39,42].
6. *On sharding protocols* Similar to layer-2 blockchain solutions, sharding protocols [41] also tackle the scalability issue of blockchain. The idea of sharding is to partition the blockchain state into multiple shards. Each shard processes a set of transactions; therefore, all shards can process the transactions parallelly and hence increases the blockchain throughput. The majority of the sharding protocols are built on the top of the Bitcoin blockchain, and some are built for the Ethereum blockchain. A sharding protocol deals with challenges involving the shard assignment to validators, transaction assignment to shard, and intra-shard consensus. A DoS attack can be mounted on sharding protocol by flooding a single shard which becomes the bottleneck for the whole system. A recent work [27] studies the DoS-attack on sharding protocols and proposes a Trusted Execution Environment (TEE) based countermeasure.
7. *On commit-chain operator* A commit-chain [23] is an off-chain scaling solution where the transactions are performed off-chain by a non-custodial and untrusted operator. The operator commits the balances of users periodically to the blockchain by computing a checkpoint and feeding it to an on-chain smart contract. The scheme involves users publishing challenges to the smart contract in case of a dispute with the operator, which imposes a drawback

where a malicious user can flood the smart contract with unwarranted challenges. Another significant issue is the operator being a central entity can become a victim of a DoS attack, resulting in collapsing the whole system.

8. *On smart contract* A smart contract is a transaction protocol in blockchain that takes actions according to the terms of the contract. In the Ethereum blockchain, each block has a maximum gas limit that is spent by executing a smart contract, and exceeding the gas limit causes a DoS attack. An attacker can mount a DoS attack on smart contract [4] in several possible ways such as: 1) By sending a computationally intensive transaction to a contract thus preventing other transactions from being included in a block; 2) By adding a couple of refund addresses at once that can end up smart contract exceeding the gas limit while refunding to those addresses; 3) By unexpected revert of refund to a legitimate user by using fallback function. A recent work [35] shows a method to detect DoS attacks caused due to unexpected revert in Ethereum smart contract. An example of a DoS attack on a smart contract is an auction contract where an attacker can constantly call the bidding function (e.g., *bid()*), preventing other legitimate users from making their bids. In the NEO blockchain, a vulnerability allowed attackers to invoke a malicious contract that created a DoS attack by crashing each node that tried to execute the contract [37]. Moreover, a DoS attack on a smart contract triggers stopping a node from executing the functions for all the DApps it hosts.
9. *On mixing services* A mixing service is a protocol that allows a cryptocurrency user to utilize its currency anonymously. It provides unlinkability of the user's input to its output and prevents the user's identification from being revealed. There are centralized [6] and decentralized [31] mixing services. Centralized mixing services being a single-point-of-failure are more vulnerable to DoS attacks (e.g. by competing services). However, both types of mixing services suffer from DoS due to different actions of its users, such as 1) By providing inconsistent input for the shuffle, leading the whole verification step of shuffle to fail; 2) By denying to perform some required task e.g., to sign a group transaction; 3) By several participation requests in the mixing transaction pool leading to the depletion of a precomputed pool by participants [49].
10. *On consensus participants* In the blockchain, consensus participants are the major players who decide on the blockchain's new block. Therefore, consensus participants are the usual DoS target for an attacker. In deterministic leader election protocols of consensus, the leader of the consensus round can be a primary target for DoS attacks which can make the whole system halt if the leader suffers a DoS attack. Other main targets can be stakeholders in Proof of Stake consensus mechanisms that hold some stake in the system, therefore attracting an attacker to mount DoS. A DoS attack can be mounted on PBFT-based permissioned blockchains and its participants, where a DDoS attack can be launched if an adversary controls over 33 % of the replicas. As in the BFT-based blockchains, network size is known to the participants, an attacker creates the required number of Sybil replicas needed for a DoS attack. Hence, for each transaction sent by the primary, the Sybil replicas will not reply to their approvals, leading the whole system to halt.

3 DoS Mitigation Techniques for Blockchain Systems

In most of the DoS events, an attacker floods the network by creating multiple transactions in a short time period, hence maximizing his throughput. This kind of situation arises when the cost of creating a transaction is low. In most settings, these transactions are monetary payment transactions of a tiny value, but for some cases, these can be data transactions (e.g., IoT blockchain transactions). To mitigate the DoS attack, some cost should be imposed on the attacker to slow down or stop unnecessary requests in the blockchain system. Hence, following, we present the DoS mitigation techniques in the blockchain ecosystem.

Blockchain Ecosystem	**Applicable Solutions**
Cryptocurrency Wallets	Client Puzzle (Inside Smart Contract)
Cryptocurrency Exchange Services	Client Puzzle (On Exchange Clients)
Memory Pools	Fee-based Approach/NI-Client Puzzle
Mining Pools	Fee-based Approach/NI-Client Puzzle
Layer-2 Blockchain Protocols	Fee-based Approach
Sharding Protocols	Fee-based Approach
Commit-chain Operator	Client Puzzle (On Commit-chain Users)
Smart Contract	Client Puzzle (Inside Smart Contract)
Mixing Services	Fee-based Approach/NI-Client Puzzle
Consensus Participants	Client Puzzle (On Participant Registration)

Table 1. DoS Mitigation Techniques in Blockchain Ecosystem

- *Client Puzzles* Client puzzles are one of the most effective prominent techniques to defend against DoS attacks. In a client puzzle, a client has to solve a puzzle before being granted access to a service or a resource by a server. The initial introduction of the client puzzle was given by Dwork and Naor [13] to combat the spam attacks. Client puzzles can be categorized into different types based on the resource used by the client for solving the puzzle such as number of CPU cycles or a number of memory access, quantifying CPU-bound puzzles [5] and memory-bound puzzles [1] respectively. Several client puzzles such as Time-lock puzzles [29], Hash-chain [24] and Equihash [7] are employed in the blockchain ecosystem. A client puzzle scheme can be *Interactive* where server creates the puzzle for the client or *Non-Interactive* (NI) where the client creates a puzzle, solves the puzzle and sends it to the server.
- *Fee-based Approach* In many events of DoS attack, to disincentivize an attacker an extra or minimum fee can be introduced in the blockchain ecosystem. This fee can be of different types based on the underlying blockchain system. The fee can be a mining fee in mining pools, a mixing fee in mixing services, a transaction fee in transaction pools, a relay fee in a blockchain network, a registration fee for user registration (e.g. a user of a permissioned blockchain), etc. Therefore, with the introduction of a minimum fee, launching a DoS attack becomes costlier for an attacker. However, the fee-based approach adversely affects legitimate users who do not want to pay this minimum amount of fee.

Table 1 presents the possible DoS mitigation solutions for corresponding blockchain ecosystem. Fee-based approach can be applied in almost every case but will not be favorable for all blockchain users. In the table, for layer-2 and sharding protocols, the use of client puzzle will defeat the purpose of scalability due to its time consumption, therefore fee-based approach is a more viable option. For memory pools, mining pools, and mixing services, non-interactive client puzzle schemes can be applied where the miner/user presents a verifiable puzzle and its solution for the inclusion of its new transaction (Rewarding puzzle solution in case of mining pool). Apart from the above described techniques, other mechanisms such as packet filtering techniques or DoS protection services e.g. Incapsula can be used for DoS mitigation in some blockchain contexts.

3.1 VDF-based DoS-resistant Protocol

Most of the existing client puzzles lack public verifiability, non-parallelizability, non-interactivity, and easy verification. Therefore, the initial introduction of VDF [8] as a moderately hard function can be configured as a client puzzle for DoS mitigation achieving all these properties. A VDF can be described as a function $f : \mathcal{X} \rightarrow \mathcal{Y}$ which takes a predefined number of steps T to compute the output $y \in \mathcal{Y}$, given an input $x \in \mathcal{X}$ and a polynomial number of processors. Furthermore, the verification of the output is exponentially easy. VDF produces a unique output that is efficiently and publicly verifiable. There have been a few constructions of VDF. We employ the Wesolowski VDF scheme [43] to construct our client puzzle due to its fast verification and short proof size properties.

We define an Interactive VDF client puzzle, where a server $\mathcal{S}$ creates a puzzle p and asks for solution s of the puzzle from the client $\mathcal{C}$ before giving access to its resource. In the following construction, $\mathcal{K}$ is a key space, $\mathcal{P}$ is a puzzle space, $\mathcal{O}$ is a solution space, $\mathcal{D}$ is a puzzle difficulty space, and $\mathcal{I}$ is a puzzle input space.

- $\mathsf{Setup}(1^\lambda)$: Select $\mathcal{K} = \varnothing, \mathcal{D} \subseteq \mathbb{N}, \mathcal{P} \subseteq \{0,1\}^*, \mathcal{O} \subseteq \{0,1\}^*, \mathcal{I} \subseteq \{0,1\}^*$. Generate a group $\mathbb{G}$ of unknown order, an RSA modulus N, a hash function $H : \{0,1\}^* \rightarrow \mathbb{G}$ and $\mathcal{D} \leftarrow T$. Set $param \leftarrow (\mathcal{P}, \mathcal{O}, \mathcal{D}, \mathcal{I})$ and $pp \leftarrow (\mathbb{G}, N, H, T)$, return $(param, pp)$.
- $\mathsf{GenPuz}(T, i, pp)$: Server runs this algorithm to create a puzzle for the client. It generates an input $i \in \mathcal{I}$ for VDF-evaluation, samples $l \xleftarrow{\$} Primes(\lambda)$. Return a puzzle $p = l$ to the client.
- $\mathsf{FindSol}(i, p, pp)$: Client runs this algorithm to solve the puzzle p. Client computes $g = H(i)$, further computes $y \leftarrow g^{(2^T)} \bmod N$. It computes q, r such that $2^T = ql + r$ where $0 \leq r < l$, and computes a proof $\pi = g^q$. Send a solution $s = (y, \pi)$ to the server.
- $\mathsf{VerSol}(i, p, s, pp)$: Server computes $r \leftarrow 2^T \bmod l$ and accepts if $g, y, s \in \mathbb{G}$ and $y = \pi^l g^r \bmod N$.

An Interactive VDF-based DoS-resistant protocol can be designed using client puzzle as depicted in Figure 1. The protocol construction follows from the Stebila et al. [38]. To define this interactive protocol, we assume server and client have

public identities $ID_{\mathcal{S}}$ and $ID_{\mathcal{C}}$. Our VDF-based client puzzle can also be made Non-Interactive where the client constructs a puzzle and its solution. The client and server share a common source of randomness (e.g. random beacon). The client creates publicly verifiable puzzles using randomness. Further, the non-interactive VDF client puzzle can be transformed into a DoS-resistant protocol that can be efficiently applied in the blockchain ecosystem during DoS events.

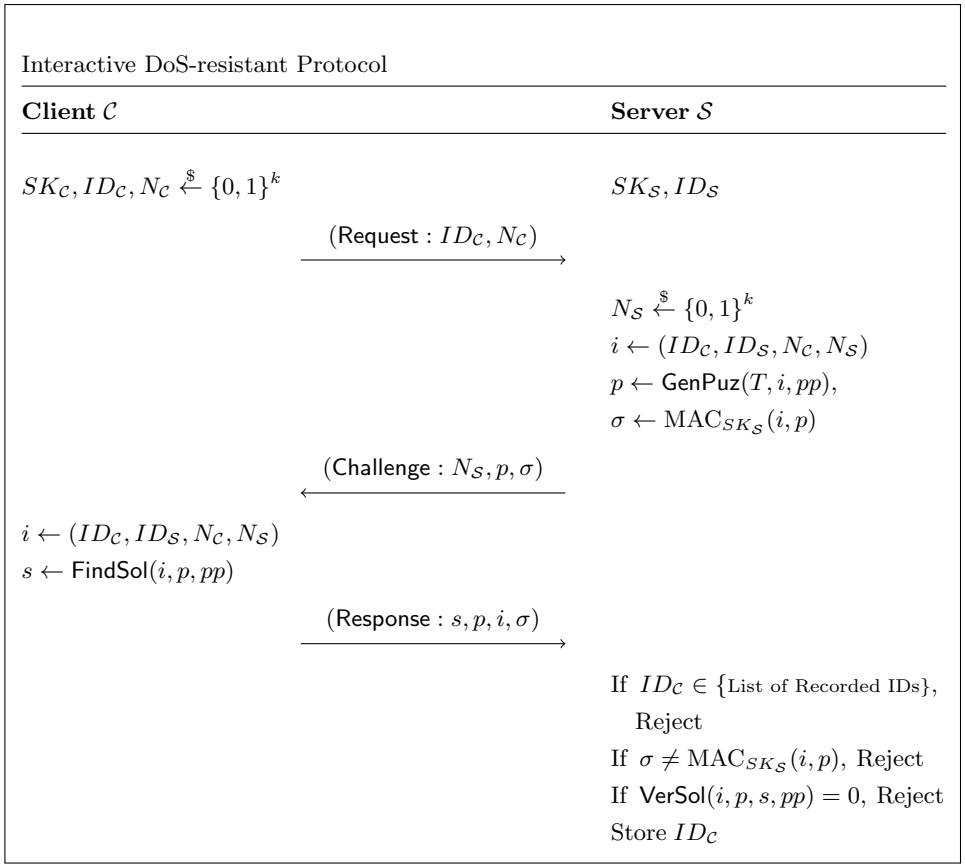

Fig. 1. Interactive DoS-resistant Protocol

Following the implementation study of VDF [3], for 128-bit security and the difficulty between 2^{16} to 2^{20}, our DoS-resistant protocol can be efficiently employed for DoS mitigation in the blockchain. With the aforementioned setting, the running time for FindSol, VerSol algorithms are in order of minutes and order of milliseconds respectively. The verification time on the server side can be further optimized using Dimitrov's multiexponentiation method [11]. As a future work, we will put a demonstration of a proof-of-concept and initial experiments with Wesolowski VDF for DoS mitigation.

4 Conclusion

In this work, we offered a thorough study of DoS attacks in the blockchain ecosystem. To the best of our knowledge, this is the first investigation in the context of blockchain. As the frequency and intensity of DoS attacks are increasing rapidly, it raises a concern about efficient detection and mitigation techniques. Therefore, we listed out main mitigation approaches which can be used for DoS mitigation in the blockchain ecosystem. We also identify verifiable delay function as an effective primitive to mitigate DoS attacks. A proper construction of non-interactive VDF puzzle and experimental results will be provided in the continuation of this work. This paper will help academic and industrial researchers to study the possible venues and impact of the DoS attack in the blockchain context and to improve upon the existing solutions.

References

1. Abadi, M., Burrows, M., Manasse, M., Wobber, T.: Moderately hard, memory-bound functions. ACM Transactions on Internet Technology **5**(2), 299–327 (2005)
2. Abhishta, A., Joosten, R., Dragomiretskiy, S., Nieuwenhuis, L.J.M.: Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange. In: 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). pp. 379–384 (2019)
3. Attias, V., Vigneri, L., Dimitrov, V.: Implementation Study of Two Verifiable Delay Functions. IACR Cryptol. ePrint Arch. **2020**, 332 (2020)
4. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on ethereum smart contracts (sok). In: Maffei, M., Ryan, M. (eds.) Principles of Security and Trust. pp. 164–186. Springer Berlin Heidelberg, Berlin, Heidelberg (2017)
5. Back, A., et al.: Hashcash - a denial of service counter-measure. ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf (2002)
6. Bao, Z., Shi, W., Kumari, S., Kong, Z.y., Chen, C.M.: Lockmix: a secure and privacy-preserving mix service for Bitcoin anonymity. International Journal of Information Security pp. 1–11 (2019)
7. Biryukov, A., Khovratovich, D.: Equihash: Asymmetric proof-of-work based on the generalized birthday problem. Ledger **2**, 1–30 (2017)
8. Boneh, D., Bonneau, J., Bünz, B., Fisch, B.: Verifiable delay functions. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology – CRYPTO 2018. pp. 757–788. Springer International Publishing, Cham (2018)
9. CoinMarketCap: Total market capitalization. `https://coinmarketcap.com` (May 2021), [Online; accessed 26-May-2021]
10. Crawley, J.: UK Crypto Exchange EXMO Offline Amid DDoS Attack. `https://tinyurl.com/u8kk94ry` (Feb 2021), [Online; accessed 08-June-2021]
11. Dimitrov, V.S., Jullien, G.A., Miller, W.C.: Complexity and fast algorithms for multiexponentiations. IEEE Transactions on Computers **49**(2), 141–147 (2000)
12. Douligeris, C., Mitrokotsa, A.: Ddos attacks and defense mechanisms: classification and state-of-the-art. Computer Networks **44**(5), 643 – 666 (2004)
13. Dwork, C., Naor, M.: Pricing via processing or combatting junk mail. In: Annual International Cryptology Conference. pp. 139–147. Springer (1992)

14. Eduardo A. Sousa, J., Oliveira, V.C., Almeida Valadares, J., Borges Vieira, A., Bernardino, H.S., Moraes Villela, S., Dias Goncalves, G.: Fighting Under-price DoS Attack in Ethereum with Machine Learning Techniques. ACM SIGMETRICS Performance Evaluation Review **48**(4), 24–27 (2021)
15. Explica.co: Cryptocurrency : Wasabi bitcoin wallet servers suffered DDoS attack. `https://tinyurl.com/s6sbunam` (June 2021), [Online; accessed 10-June-2021]
16. Fadilpasic, S.: Disclosed: Ethereum 'Lived' With a Major Threat for 18 Months. `https://tinyurl.com/h7478aej` (May 2021), [Online; accessed 07-July-2021]
17. Feder, A., Gandal, N., Hamrick, J., Moore, T.: The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. Journal of Cybersecurity **3**(2), 137–144 (2017)
18. Fuller, B., Khan, J.: CVE-2018-17145: Bitcoin Inventory Out-of-Memory Denial-of-Service Attack. https://invdos.net/paper/CVE-2018-17145.pdf (2020)
19. Gasti, P., Tsudik, G., Uzun, E., Zhang, L.: DoS and DDoS in Named Data Networking. In: 2013 22nd International Conference on Computer Communication and Networks (ICCCN). pp. 1–7 (2013)
20. Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., Gervais, A.: Sok: Layer-two blockchain protocols. In: Financial Cryptography and Data Security. pp. 201–226. Springer International Publishing, Cham (2020)
21. Gupta, B., Badve, O.P.: Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. Neural Computing and Applications **28**(12), 3655–3682 (2017)
22. Higgins, S.: Bitcoin Mining Pools Targeted in Wave of DDoS Attacks. `https://tinyurl.com/5jew979z` (March 2015), [Online; accessed 07-July-2021]
23. Khalil, R., Zamyatin, A., Felley, G., Moreno-Sanchez, P., Gervais, A.: Commit-Chains: Secure, Scalable Off-Chain Payments. Tech. rep., Cryptology ePrint Archive, Report 2018/642 (2018)
24. Mahmoody, M., Moran, T., Vadhan, S.: Publicly verifiable proofs of sequential work. In: Proceedings of the 4th conference on Innovations in Theoretical Computer Science. pp. 373–388 (2013)
25. Mirkin, M., Ji, Y., Pang, J., Klages-Mundt, A., Eyal, I., Juels, A.: BDoS: Blockchain Denial-of-Service. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. p. 601–619. CCS '20, ACM, NY, USA (2020)
26. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf (2009)
27. Nguyen, T., Thai, M.T.: Denial-of-service vulnerability of hash-based transaction sharding: Attacks and countermeasures. arXiv preprint arXiv:2007.08600 (2020)
28. Praitheeshan, P., Pan, L., Doss, R.: Security Evaluation of Smart Contract-Based On-chain Ethereum Wallets. In: International Conference on Network and System Security. pp. 22–41. Springer (2020)
29. Rivest, R.L., Shamir, A., Wagner, D.A.: Time-lock puzzles and timed-release crypto. Massachusetts Institute of Technology, Laboratory for Computer Science (1996)
30. Rodrigues, B., Bocek, T., Stiller, B.: Multi-domain ddos mitigation based on blockchains. In: Tuncer, D., Koch, R., Badonnel, R., Stiller, B. (eds.) Security of Networks and Services in an All-Connected World. pp. 185–190. Springer International Publishing, Cham (2017)
31. Ruffing, T., Moreno-Sanchez, P., Kate, A.: Coinshuffle: Practical decentralized coin mixing for Bitcoin. In: European Symposium on Research in Computer Security. pp. 345–364. Springer (2014)

32. Saad, M., Njilla, L., Kamhoua, C., Kim, J., Nyang, D., Mohaisen, A.: Mempool Optimization for Defending Against DDoS Attacks in PoW-based Blockchain Systems. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). pp. 285–292. IEEE (2019)
33. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., Mohaisen, A.: Exploring the attack surface of blockchain: A systematic overview. arXiv preprint arXiv:1904.03487 (2019)
34. Saad, M., Thai, M.T., Mohaisen, A.: POSTER: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization. In: Proceedings of the 2018 on Asia Conference on Computer and Communications Security. pp. 809–811 (2018)
35. Samreen, N.F., Alalfi, M.H.: SmartScan: An approach to detect Denial of Service Vulnerability in Ethereum Smart Contracts. preprint arXiv:2105.02852 (2021)
36. Singh, R., Tanwar, S., Sharma, T.P.: Utilization of blockchain for mitigating the distributed denial of service attacks. Security and Privacy **3**(3), e96 (2020). https://doi.org/https://doi.org/10.1002/spy2.96
37. Sotnichek, M.: NEO Smart Contract Vulnerabilities: DoS Vulnerability. `https://tinyurl.com/faxjbby5` (October 2018), [Online; accessed 07-July-2021]
38. Stebila, D., Kuppusamy, L., Rangasamy, J., Boyd, C., Gonzalez Nieto, J.: Stronger difficulty notions for client puzzles and denial-of-service-resistant protocols. In: Kiayias, A. (ed.) Topics in Cryptology – CT-RSA 2011. pp. 284–301. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
39. Tochner, S., Zohar, A., Schmid, S.: Route Hijacking and DoS in Off-Chain Networks, p. 228–240. ACM, New York, NY, USA (2020)
40. Vasek, M., Thornton, M., Moore, T.: Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. In: Böhme, R., Brenner, M., Moore, T., Smith, M. (eds.) Financial Cryptography and Data Security. pp. 57–71. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)
41. Wang, G., Shi, Z.J., Nixon, M., Han, S.: SoK: Sharding on blockchain. In: 1st ACM Conference on Advances in Financial Technologies. pp. 41–61 (2019)
42. Weintraub, B., Nita-Rotaru, C., Roos, S.: Exploiting Centrality: Attacks in Payment Channel Networks with Local Routing (2020)
43. Wesolowski, B.: Efficient verifiable delay functions. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019. pp. 379–407. Springer International Publishing, Cham (2019)
44. Wilcke, J.: The Ethereum network is currently undergoing a DoS attack. `https://tinyurl.com/ww6kp2nu` (2016), [Online; accessed 07-July-2021]
45. Wood, G., et al.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper **151**(2014), 1–32 (2014)
46. Woolf, N.: DDoS attack that disrupted internet was largest of its kind in history, experts say. The Guardian **26** (2016)
47. Wu, S., Chen, Y., Li, M., Luo, X., Liu, Z., Liu, L.: Survive and Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools. IEEE/ACM Transactions on Networking **28**(2), 874–887 (2020)
48. Zheng, R., Ying, C., Shao, J., Wei, G., Yan, H., Kong, J., Ren, Y., Zhang, H., Hou, W.: New Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools with Defence Cost. In: International Conference on Network and System Security. pp. 567–580. Springer (2019)
49. Ziegeldorf, J.H., Matzutt, R., Henze, M., Grossmann, F., Wehrle, K.: Secure and anonymous decentralized Bitcoin mixing. Future Generation Computer Systems **80**, 448–466 (2018)