Blockchain-Based Detection and Analysis of DDoS Attacks in Decentralized Networks

MSc Research Project
Cyber Security

Rutwik Sayankar
Student ID: x23213841

School of Computing
National College of Ireland

Supervisor: Dr. Rohit Verma

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Rutwik Sayankar
Student ID:	x23213841
Programme:	Cyber Security
Year:	2024
Module:	MSc Research Project
Supervisor:	Dr. Rohit Verma
Submission Due Date:	12/12/2024
Project Title:	Blockchain-Based Detection and Analysis of DDoS Attacks in Decentralized Networks
Word Count:	5881
Page Count:	20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Rutwik Arvind Sayankar
Date:	27th January 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Blockchain-Based Detection and Analysis of DDoS Attacks in Decentralized Networks

Rutwik Sayankar
x23213841

Abstract

As most of the people using blockchain technology for secure and decentralized transactions, highlight the need of strong security measures against cyber threats. This research explores the impact of distributed denial-of-service (DDoS) attacks on the blockchain network. This analysis is focused on how DDoS attacks impact key performance analysis metrics like block processing time, CPU usage and network traffic. Also, this study examines the impact of various kind of traffic ranging from malicious ones like DDoS attacks to normal traffic, on the performance of blockchain functionality. This is done by using experiments with several validator nodes, member nodes of blockchain. According to the findings of this research, DDoS attacks increase block processing time, CPU usage and disturb network traffic, which highlights the vulnerability in the blockchain infrastructure. This research uses statistical analysis and machine learning to evaluate these effects and offers some methods to recognize threats. The results of this research offer valuable insights that can be helpful for researchers and people who work in the cybersecurity field. It also highlights the need for advanced security measures and regular monitoring within blockchain frameworks. This research suggests conducting additional studies by using advanced machine learning techniques to analyze the efficiency and scalability of the system and make blockchain safer.

Keywords : Permissioned Blockchain, Distributed Denial of Service (DDoS), Machine Learning, Quorum, Blockchain security

1 Introduction

In this developing world of cybersecurity, Distributed Denial of Service (DDoS) attacks remain a serious threat to the reliability and availability of decentralized networks across various sectors. These decentralized systems are designed to eliminate the single points of failure like the centralized structure of a network but they introduce unique vulnerabilities.Correia et al. (2024) DDoS attacks are dangerous for this type of network, as it has the ability to exploit multiple nodes of the network simultaneously. Traditional defense mechanisms against DDoS attacks like centralized models and statistical methods faced some challenges in scalability, data privacy and compatibility with the decentralized nature of blockchain. The approach of gathering data in a centralized location proved ineffective as models struggled to adapt continuously evolving attack patterns leads to resource waste because of inefficient data processing. These limitations highlight the need for adaptable and decentralized approaches like integrating blockchain with machine learning.Saveetha et al. (2024) This paper presents a new framework that integrates machine learning (ML) and blockchain technology to improve the detection and validation of DDoS activities. By focusing on the enhancement of security as well as transparency, this integration tackles various critical issues faced by DDoS defense mechanisms. This integration supports quick anomaly detection, decentralized incident validation and generates tamper proof logs for actions taken against recognized threats.Xu et al. (2024)

Decentralized networks have many security vulnerabilities because of their open and distributed architecture. Without a centralized authority, these networks can easily be attacked by DDoS attack, where attackers can target multiple nodes to effectively interrupt the service continuity. Such kind of interruptions can greatly affects network performance and can cause considerable financial as well as reputational losses. This situation highlights the importance of solid security protocols to maintain operational integrity and defend user's confidence in decentralized infrastructures.Ibrahim et al. (2022)Abdullah and Hussein (2024)

Quorum is a permissioned blockchain platform based on Ethereum. It gives effective solutions for applications that require a combination of high transparency and strong privacy measures. Quorum blockchain improves security in decentralized environments by implementing advanced consensus protocols like Byzantine Fault Tolerance (BFT) and RAFT. These mechanisms make sure that all transactions and blocks are verified by trusted nodes. This helps to minimize risk of malicious activities and makes sure the reliability of network functionality.Baliga et al. (2018)

Previous researches have shown that the blockchain and machine learning can be effective in defending against cyber threats. However, they often face some challenges related to scalability, resource demands and deployment difficulties. This research addresses these challenges by integrating machine learning model with the Quorum blockchain. This integration not only uses strong security and privacy features of the Quorum blockchain but also enhances the precision and speed of DDoS detection efficiency. Also, the privacy feature of the Quorum blockchain makes sure that the transaction details remain confidential among the involved parties, which is an aspect that previous research often overlooked.

The following Research Question is motivated by the previously mentioned research problems :

How can the integration of blockchain technologies and machine learning improve the security and transparency in the detection and analysis of DDoS attacks within decentralized networks?

This research proposes an innovative approach that merges the predictive strengths of machine learning with secure and decentralized features of the Quorum blockchain to tackle DDoS attacks. This approach provides scalable, efficient and secure methods for enhancement of defenses against DDoS attacks. It also gives useful insights into the wider field of cybersecurity by providing reliable and practical solutions to strengthen the resilience of decentralized systems.Pawar et al. (2024)

2 Related Work

2.1 Importance of DDoS detection in Blockchain Systems

Blockchain technology is recognized for its decentralized structure, transparency and resilience against tampering Dong et al. (2023). However, it can still be affected by threats like Distributed Denial of Service (DDoS) attacks, which can significantly disrupt its network operations as well as performance. These attacks saturate the blockchain with excessive malicious traffic, then take advantage of vulnerabilities that are present themselves within its peer-to-peer (P2P) framework Wani et al. (2021). Because of its decentralized architecture of blockchain, it creates complications in the implementation of effective mitigation strategies compared to centralized architecture, where a single authority can implement strict security protocols.

In permissionless or public blockchains like Bitcoin and Ethereum, the open nature of these networks presents an easy target for DDoS attacks. An evident case in point is the Ethereum EXTCODESIZE[1] attack, where attackers exploited vulnerabilities in opcodes to slow down miner's block processing ability Xu et al. (2024). This resulted in serious disruptions to network communication. Such events highlight the urgent necessity for advanced detection and mitigation solutions to prevent economical issues and to defend the operational integrity of blockchain systems.

Even in permissioned blockchains, which are characterized by their controlled environments, the risk of DDoS attacks remains a significant issue. These systems depend on a limited set of predefined validators for reaching consensus, which makes them particularly vulnerable to targeted attacks. Evidence shows how malicious traffic can overwhelm consensus nodes. It also highlights the importance of strengthening these systems as blockchain technology gains across various sectors, including finance, supply chain and healthcare Nasir et al. (2024).

Li et al. (2024) developed a methodology to detect anomalous traffic in permissioned blockchain by using two-layer of GRU model. This approach begins with the analysis of traffic patterns associated with DDoS attacks on smart contracts. Here random forest model is used to evaluate the features to obtain an importance ranking of features. This ranking is used to create a dataset that trains the GRU model, which combines the standard GRU model with the encoder-decoder framework to improve the detection effectiveness. This approach shows the effectiveness in the detection of DDoS attacks by highlighting the importance of creating security measures for permissioned blockchain environments.

2.2 Exploring Modern Research Trends

To address DDoS threats in blockchain systems, researchers are exploring various methods, especially the integration of machine learning with blockchain technology. The strategies can be widely classified into some primary categories : statistical detection methods, machine learning-based detection techniques and blockchain-enhanced mitigation strategies.

[1] `https://blog.ethereum.org/2016/09/22/transaction-spam-attack-next-steps`

2.2.1 Statistical Methods & Machine Learning Techniques

The traditional approach to DDoS detection often relies on statistical analysis of network traffic patterns. The main goal of these techniques is to identify anomalies like unusual traffic volumes or frequencies. However, their effectiveness becomes weak when faced with evolving attack patterns and increasingly sophisticated malicious actors or attackers Pawar et al. (2024) Xu et al. (2024).

Machine learning algorithms have come up as a powerful alternative due to their capacity to adapt according to the changing attack vectors. Supervised machine learning models like Support Vector Machines (SVM) and Random Forests have been employed to differentiate between benign and malicious traffic. More advanced approaches involve deep learning models like Long Short-Term Memory (LSTM) networks and Gated Recurrent Units (GRU). These models are effective at detecting temporal patterns in traffic data Pawar et al. (2024). Similarly, Jawahar et al. (2024) utilized the CICDDoS2019 dataset to evaluate multiple classifiers, finding ANN to outperform others with an accuracy of 98.57%. This high accuracy highlights the potential of deep learning for real-time traffic analysis in blockchain environments.

Federated learning presents another innovative approach, which allows multiple blockchain nodes to collaboratively train detection models while protecting raw data privacy. However, depending on centralized aggregation nodes introduces potential vulnerabilities, particularly in fully decentralized environments Xu et al. (2024). Also in the same way, Saveetha et al. (2024) proposed the application of federated learning frameworks to enhance collaborative model training while preserving data privacy. This approach addressed the challenges of data centralization by enabling individual nodes to train models locally before measuring them into a global model. However, federated learning models are vulnerable to attacks, where malicious nodes compromise the global model's integrity. This limitation points out the need for secure integration with blockchain technologies to improve the model's reliability and trustworthiness.

2.2.2 Mitigation Strategies improved by Blockchain

The integration of blockchain technology with DDoS mitigation techniques offers distinct advantages, like the ability to make decentralized decision and a maintain tamper-proof record. There has been current research going on to explore synergies in depth :

1. Software-Defined Networking (SDN) Solutions: By merging SDN with blockchain technology, researchers have managed to distribute detection and mitigation responsibilities across multiple nodes, so that single points of failure are minimized. The immutable nature of blockchain simplifies the logging of attack events and responses, which helps to maintain accountability Pawar et al. (2024).

2. Consensus Mechanisms: Protocols such as Practical Byzantine Fault Tolerance (PBFT) and Quorum Byzantine Fault Tolerance (QBFT) are very important in maintaining network security during attacks, which makes sure that malicious validators cannot compromise the blockchain's integrity Correia et al. (2024)Nasir et al. (2024). Even though these approaches have potential, they frequently encounter challenges related to decentralization, scalability, and computational demands.

2.2.3 Anomaly Detection within Permissioned Blockchains

Research targeted at DDoS mitigation in permissioned blockchains has largely revolved around developing anomaly detection techniques suited to their controlled operational environments. Models based on GRU have proven effective in detecting malicious internet traffic by analyzing parameters like packet size and transmission frequency. While these approaches have improved detection accuracy, they require robust integration with consensus protocols to make sure timely responses Pawar et al. (2024) Nasir et al. (2024).

2.3 Securing Permissioned Blockchain Frameworks

Unlike public blockchains like Ethereum, permissioned blockchains are specifically designed for particular organizational applications, providing enhanced control, privacy and operational efficiency. However, these systems depend on a limited number of validators in the system, leading to unique security vulnerabilities.

One major concern is the vulnerability of consensus nodes to targeted DDoS attacks. The vulnerability of these systems increases with fewer validators, which make them easier to disrupt, especially during long lasting DDoS attacks. Traditional consensus mechanisms like PBFT may struggle to maintain reliability under such conditions Nasir et al. (2024)

To mitigate these vulnerabilities, researchers have proposed advanced consensus frameworks like QBFT, which enhances fault tolerance by allowing the network to function even when a subset of validators acts maliciously. Also, because of controlled nature of permissioned blockchains, allows the deployment of machine learning models for real-time traffic analysis, which enhance their security measures Correia et al. (2024)Nasir et al. (2024).

2.4 Research Niche

This research addresses critical issues in the existing literature by focusing on the following areas:

1. **Transparent Detection Logging:**
   Many current systems lack effective means for securely recording detection results. The proposed framework uses Quorum blockchain to ensure a tamper-proof audit trail.
2. **Enhanced Fault Tolerance:**
   By adopting QBFT consensus, the framework improves resilience against attacks targeting consensus nodes, which is a common vulnerability in permissioned blockchains.
3. **Dynamic Detection Capabilities:**
   The integration of machine learning with blockchain technology allows for real-time responsiveness, overcoming the limitations associated with static detection methodologies.

2.5 Addressing Research Gaps

The proposed framework aims to address the following research deficiencies mentioned in table 1:

Research Gap	**Existing Research**	**Proposed Solution**
Insufficient Transparency in Detection Logging	Limited adoption of blockchain technology for secure, transparent documentation of logs. Wani et al. (2021) Xu et al. (2024)	Utilizes Quorum blockchain to create immutable, secure logs.
Scalability and Decentralization Constraints	PBFT mechanisms may become vulnerable during large scale DDoS attacks.Correia et al. (2024)Nasir et al. (2024)	QBFT consensus enhances scalability and robustness against attacks.
Inefficient Real Time Detection	Existing solutions usually depends on post incident analysis Pawar et al. (2024)	Integrates Random Forest for dynamic, real-time traffic monitoring.

Table 1: Proposed Framework Research Gaps and Solutions (Table 1)

3 Methodology

This section explains the structured methodology used to integrate machine learning with blockchain technology. The main goal is to establish a secure and decentralized framework for detection and validation of DDoS attacks. This research covers the entire process, starting from data preparation to the system evaluation while ensuring precision, effectiveness and resilience at each step.

The key part of methodology is thorough data preparation to maintain the quality and integrity of the dataset used for training the machine learning model. This phase involves cleaning of data to remove incomplete or inaccurate entries, which enhances the reliability of the model. Then the selection of relevant features is also important to minimize computational load to reduce the risk of overfitting. The features are standardized to the scale range of 0 to 1 in order to help better model prediction. These methods are similar to the methodologies proposed by researchers like Pawar et al. (2024) and Abdullah and Hussein (2024). These methods highlighted the importance of integrity and quality in data used for model training.

It is important to use an effective detection model, especially during Distributed Denial of Service (DDoS) attacks. This research thoroughly examined several models with their unique strengths and weaknesses. Even though Random Forest is the best choice, there are several other models having unique characteristics and impressive outcomes. Support Vector Machines (SVMs) are well known for handling large amounts of data easily, but they struggle to perform well when the dataset is too large. Logistic regression is user-friendly, but it struggles with complex patterns that have non-linear decision boundaries. Neural networks are excellent at recognizing complex patterns, but they are dependant on a certain amount of data and advanced computer resources, which makes them less feasible. While Random Forest is based on several advantages that are dynamic and upgrading the nature of security. Random Forest effectively prevents the risk of overfitting in complicated models. This is very important for maintaining strong performance against changing DDoS attack methods.

Also, based on previous evidence that supports the use of strong classifiers within cybersecurity, the Random Forest classifier is used Li et al. (2024). This classifier is selected for its effectiveness and resilience to manage large datasets with complex patterns without the need of extra preparation. It also highlights the most important features used for predictions and improves transparency in the decision making of model. These factors are very important for the detection of DDoS attacks.

A flask application is developed for the deployment of a machine learning model and creation of a user interface for predictions and result visualization. It is recognized for its lightweight and adaptable nature, which is used to create an application that works as an interface for DDoS attack detection. This framework allows the creation of endpoints that collects network traffic data, which uses predictions from the trained model and responds instantly. It also allows the development of visualization endpoints that dynamically created and present statistical representations that help to enhance the understanding of model efficiency.

Using security features of the Quorum blockchain as explained by Nasir et al. (2024) , enables secure and immutable logging of all predictions. This integration enhances data integrity and confidentiality for enterprise level businesses, which need decentralized and tamper-proof logging mechanisms.

According to Correia et al. (2024), the selection of consensus mechanisms like QBFT and PoA is determined by their ability to provide balance between fault tolerance and operational efficiency. These mechanisms are important for maintaining system performance and offer strong security against node failures or malicious attacks. All these things are done while maintaining high transaction throughput.

For ongoing performance assessment, this approach uses Prometheus and Grafana. These tools helps in monitoring key metrics like transaction throughput and consensus efficiency.

4 Design Specification

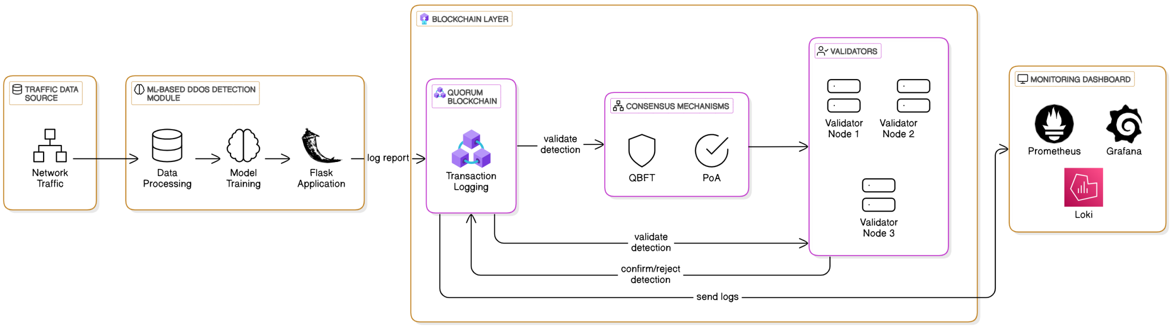


Figure 1: Architecture of integration of ML and Blockchain for DDoS Detection

This section describes the system that uses machine learning (ML) and blockchain technology to efficiently detect, validate and monitor Distributed Denial of Service (DDoS) attacks securely and transparently. The design architecture as shown in figure 1 , this system has four key components the traffic data source, the machine learning (ML) based DDoS detection module, the blockchain infrastructure and the monitoring dashboard. A detailed description of each component and its importance to fulfilling system requirements is mentioned below.

4.1 Traffic Data Source:

The basic part of the system is the traffic data source, which collects network traffic data that includes payload information and protocol metadata related to network activity. This raw data is very important for finding out DDoS attack patterns. The system uses the CIC-DDoS2019 [2] dataset as the primary source of network traffic data. This dataset provides a controlled and reproducible environment for experimentation and validation.

4.2 ML Based DDoS Detection Module:

This module is very important in the system for the detection mechanism. This module analyzes raw traffic data by using machine learning algorithms to identify DDoS attack patterns. The data processing workflow is designed to clean the data, normalize values and extract key features like packet rates and protocol types.

Once the data is processed, machine learning models are trained to detect anomalies in network traffic that points out as DDoS attack. To ensure the accuracy of these models, they are evaluated by using performance metrics like precision, recall and F1-score. Upon identifying a DDoS attack, the module sends a detailed report containing important details like timestamps, IP addresses and confidence scores that is generated to the blockchain layer. This process is completed by using a Flask application that enables flawless integration and efficient data transfer.

4.3 Blockchain Infrastructure:

The blockchain layer plays an important role in secure, transparent and tamper-proof logging detection results. The system uses Quorum blockchain, which is a permissioned blockchain platform designed for private applications to record all detection logs as blockchain transactions. Each detection is stored as critical information, including attack metadata and detection confidence scores.

To make sure the transaction is valid, the system uses two consensus mechanisms :

1. Quorum Byzantine Fault Tolerance (QBFT) : This mechanism protects the systems against malicious nodes.

2. Proof of Authority (PoA) : This is a lightweight consensus mechanism that relies on trusted validator nodes for transaction approval.

This blockchain functionality not only secures detection records but also provides agreement among validators related to the authenticity of each reported incident.

Validator nodes plays an important role in examining detection logs to confirm the authenticity of reported attacks. These nodes cross verify the detection reports against a set of established criteria and use QBFT or PoA consensus mechanisms to reach an agreement. The system uses multiple validator nodes to improve its fault tolerance by ensuring operational continuity even when some node failures occur in the event. Once consensus is achieved, the validated logs are securely recorded on the blockchain while maintaining their integrity.

[2] https://www.unb.ca/cic/datasets/ddos-2019.html

4.4 Monitoring Dashboard:

An advanced monitoring dashboard is important for evaluation of detection accuracy and system efficiency. It combines logging and detection functionalities to deliver insights into the system's performance. This system uses Prometheus for collecting diverse information about blockchain performance, Loki for collecting logs and Grafana for visual data representation.

4.5 System Workflow:

1. Data Collection : The CIC-DDoS2019 [3] dataset is used to generate network traffic data for analysis.
2. Data Processing and Detection : The input data is cleaned and all relevant features are extracted during preprocessing to prepare it for machine learning. This processed data is then analyzed by a trained ML model to identify patterns of DDoS attacks and log the results.
3. Blockchain Logging : Detection reports are sent to the blockchain via the Flask application and recorded on the blockchain for further validation.
4. Validation : Validator nodes first review, then either approve or reject the detections findings by using established consensus mechanisms.
5. Real-Time Monitoring : The monitoring dashboards, i.e Grafana and Loki, visualize logs and key performance metrics, ensuring transparency of system performance.

4.6 Key Features:

This thorough design uses the strengths of both machine learning and blockchain technology to establish a strong, secure and scalable DDoS detection system. The blockchain component makes sure that logs should be transparent and tamper proof, while monitoring dashboards provides actionable insights in real time. Validator nodes help to make the system reliable by ensuring consensus on detection results. Collectively, these components form a strong system to address the challenges of modern network security threats.

5 Implementation

The implementation involves the development of a solid framework for the detection of Distributed Denial of Service (DDoS) attacks by using a systematic approach that covers several important phases. These phases includes the data preparation, development of a Flask application for DDoS detection, integration of Quorum blockchain for decentralized logging and performance monitoring of the blockchain. Each phase of developing the framework is carefully designed to create a secure, transparent and efficient mechanism for the detection and validation of DDoS attacks.

[3] `https://www.unb.ca/cic/datasets/ddos-2019.html`

5.1 Data Preparation

5.1.1 Data Selection

In this research the **CICDDoS2019** dataset is used, which is publicly available and it is specifically designed to represent real world DDoS attack scenarios. It contains both benign and malicious network traffic, with a variety of attack types.

5.1.2 Data Preprocessing

To make sure the best performance of the dataset for machine learning applications, several steps of preprocessing were implemented :

Feature Selection : Identifying appropriate features is important for effective anomaly detection. In this dataset, several key network traffic features like source port, destination port, total fwd packets, packet length variance, protocol type were selected based on their noticeable deviation in the network. These features were recognized based on their correlation with DDoS attack characteristics, which make sure that the model would be equipped to detect anomalies.

Data Cleaning : The dataset was checked for any missing or invalid values, which were either corrected or removed to make sure of the data integrity. To enhance the performance of a machine learning model when dealing with new, unseen traffic.

Normalization : To make it easier to compare among various data types, numerical features were normalized. This step is important as it standardizes all data points to a common scale, which helps to mitigate any potential bias in model training. Normalization is very important for certain algorithms like Random Forest, where consistent weightage across features is necessary for optimal performance.

5.1.3 Data Splitting

The dataset was divided into 80% for model training and 20% for model testing. By using 80% of the dataset for training, it provides the model with a sufficiently large set of examples for effective learning. This wide range of exposure is important for the model to learn and remember various patterns and details present in the data. The remaining 20% of the dataset is used for testing purposes, which is important for determining the model's effectiveness in predicting the new and unseen data. This configuration helps in identifying overfitting and simultaneously guards against underfitting. Also, the validation of the data enhances the significance of results, making the 80-20 split an effective principle.

5.1.4 Model Training

The **Random Forest classifier** was used for its resilience and capacity to manage huge datasets. This model was properly trained on the labeled dataset and gave a high level of accuracy in identifying DDoS attacks. The trained model was serialized and stored as a **pickle file** to reuse it in the Flask application.

5.2 Quorum Blockchain Features

Quorum blockchain is the permissioned version of the Ethereum blockchain, designed for private and enterprise level applications. The design of Quorum is useful for secure and transparent logging, helping to make decentralized decision-making processes easier that fulfill the organization's needs. Here are some features that are required for the implementation of the Quorum blockchain.

5.2.1 Node Configuration and Interaction

After deployment of the Quorum network, the nodes are automatically configured based on earlier selections.

i. Node Endpoints: Each node in the network gives a JSON-RPC endpoint for local access. For example, validator nodes are accessed at `http://localhost:8545` , while member nodes can be accessible at `http://localhost:22000` .

ii. Node Interaction : To interact with these nodes, some libraries like Web3.py can be used. The Web3.py library interacts with Quorum via the HTTP RPC endpoint (`http://localhost:8545`).

5.2.2 Monitoring and Administration Tools

To assess the effectiveness and functionality of the Quorum blockchain, multiple advanced monitoring tools have been used. These tools not only collect essential data but also enhance the understanding of the network's functionality.

i. **Prometheus** : Prometheus is a powerful monitoring solution that is designed to collect diverse information about blockchain performance. Prometheus can be accessed via `http://localhost:9090` for viewing and querying raw metrics from blockchain nodes.

ii. **Grafana** : Grafana is a visualization tool that helps to understand the data collected by Prometheus in a visual way. It allows the development of detailed dashboards that present real-time data on blockchain performance. Grafana can be accessed via `http://localhost:3000` to visualize performance metrics of the blockchain.

iii. **Loki** : Loki works as a log aggregation tool integrated with Grafana. It collects logs from all containers and gives a comprehensive overview of network activities and operational health.

These monitoring tools allows to gain a detailed understanding of Quorum blockchain's performance. These are used in enhancement in decision making and optimization of strategies.

5.3 Flask Application for DDoS Detection

In this research, one approach is introduced to deal with the DDoS attack threat through the deployment of a Flask application that uses machine learning algorithms for detection of the DDoS attacks.

5.3.1 Load Trained Model

In this step, the pre-trained Random Forest model from the pickle file, which was initially developed using a preprocessed dataset, is integrated into the **Flask** application. Once the application starts, it loads a serialized model to manage network traffic efficiently. This design eliminates the need for retraining the model and provides fast as well as efficient predictions of DDoS attacks.

5.3.2 Flask Application Features

Flask application is a structured application that offers a range of important functionalities that enhance its usability in DDoS detection.

1. Prediction Endpoint : The main feature of the application is the `/predict` endpoint. This interface accepts the characteristics of network traffic formatted in JSON. When a request is made, the Flask app uses a pretrained random forest model to analyze the input data and differentiate it as either benign or indicative of a DDoS attack. This quick evaluation is very important for organizations looking to secure their digital infrastructure.

2. Blockchain Logging : To enhance accountability and traceability, the flask app includes the logging mechanism that records prediction results to a blockchain. Each prediction is treated as a transaction, which makes sure that all data is secure and transparent. This feature not only supports security but also provides a reliable audit trail for future analysis.

3. Retrieving blockchain logs : This application also provides `/get-logs` endpoint, which allows users to fetch and decode transaction data linked with the logged predictions. By analyzing these logs, users can get all information into traffic patterns and the frequency of DDoS attacks.

4. Visualization Features : Additionally, the `/matrix` endpoint is added to display a confusion matrix, which helps to enhance user experience and provide a deep understanding of the model's performance.

5.4 Integration of Flask Application with Quorum Blockchain

5.4.1 Connecting to Quorum Blockchain

The integration of the Flask application and Quorum Blockchain node is easier with the help of the **Web3.py** library. This connection is initiated by defining the JSON-RPC endpoint of nodes, which is used as the communication bridge between the application and the blockchain. In this setup, Proof of Authority **middleware** is integrated, which ensures the compatibility between the Flask application and the Quorum blockchain.

5.4.2 Logging Predictions

In this setup, every prediction generated by the Flask application is sent to the blockchain as a transaction. Each transaction shows the result of the prediction, which is important for maintaining a tamper-proof record on the blockchain.

1. Transaction Format :

   i. The prediction result indicates whether the prediction was defined as DDoS or Benign.

   ii. Metadata includes essential information like sender's address and corresponding block number.

   iii. Each transaction is signed by using the default blockchain account, which is preconfigured in the Flask application.

2. Transaction Confirmation : To ensure reliability, the Flask application waits for a transaction receipt, which gives a confirmation that the prediction has been successfully recorded on the blockchain.

5.4.3 Retrieving Logs

The Flask application features a `/get-logs` endpoint, which is designed to get transaction data from the blockchain. This endpoint decodes the payload to get logged predictions. All entries in the log are detailed and provide significant information like:
1. Block Number, which identifies the specific block in which the transaction was logged.
2. Transaction hash, which is used to identify the log.
3. Prediction result, which provides insight into the recorded event, which is either DDoS or Benign.

5.5 Monitoring Quorum Blockchain

5.5.1 Consensus Mechanism

1. Quorum Byzantine Fault Tolerance (QBFT)

Quorum's Byzantine Fault Tolerance (QBFT) is a consensus mechanism designed to maintain reliability within distributed networks. It works through several rounds of communication processes between validators, which is important for achieving consensus. This method is especially useful in environments where reliability is very important. It supports the network in being strong against malicious actors without compromising the performance of the blockchain.

2. Proof of Authority (PoA)

Proof of Authority (PoA) provides a different approach to consensus by using a selected group of validators. This model is distinguished by its efficiency, as it uses trusted entities to validate transactions. PoA is ideally suited for scenarios where participants are known and have a good reputation. This helps with quicker decision-making and reduces the additional tasks that are typically involved with more decentralized consensus methods.

5.5.2 Monitoring Tools

1. Grafana provides real time dashboards that display metrics like transaction throughput, resource usage, block finalization time and node resource consumption.

2. Loki gives logs from blockchain nodes which are aggregated and visualized. These logs provide insights into the consensus process and transaction history.

6 Evaluation

This section deals with the detailed analysis of experimental results related to the detection of DDoS attacks through the use of blockchain technology. The evaluation discusses the practical implications of these results, which highlights the key insights that support the main research question and goals.

6.1 Average Block Processing Time

The initial experiment analyzed the time required to process blocks under diverse traffic conditions, which compares benign versus DDoS transactions across four different validators. The graph of this data clearly demonstrates the effects of DDoS attacks on block processing times. Under DDoS conditions, validators showed a fluctuation in processing delays when compared with benign scenarios.

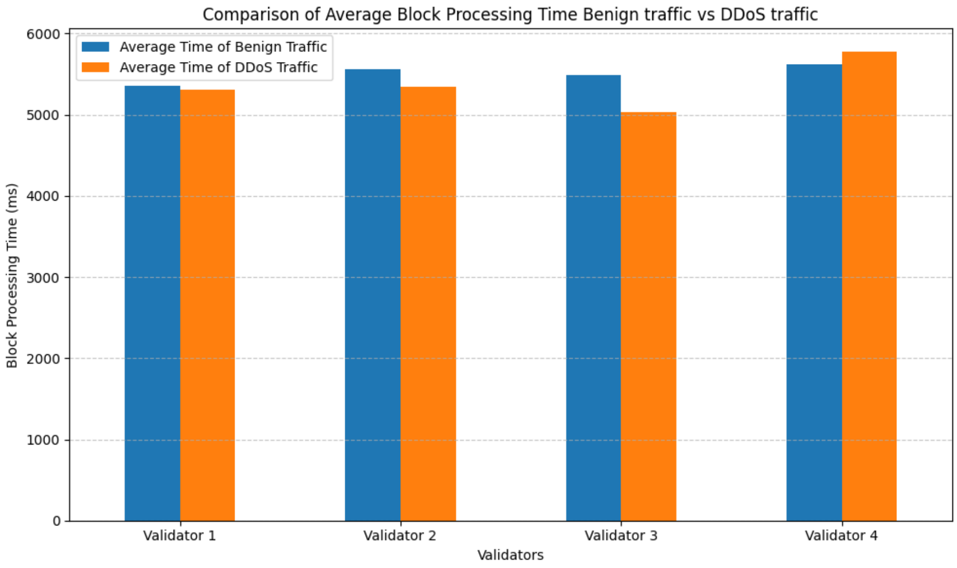


Figure 2: Comparison of Average Block Processing Time between Benign traffic and DDoS traffic

The graph shown in figure 2 clearly illustrates that the average block processing time of validators during the DDoS attack is fluctuating because of increased load on the network. While under benign traffic, the graph is relatively stable as compared to during a DDoS attack; this shows that the network is under normal load.

Validators	**Average Time of Benign Traffic (ms)**	**Average Time of DDoS Traffic (ms)**
Validator 1	5355.347107	5309.851240
Validator 2	5559.198347	5348.000000
Validator 3	5489.289256	5035.652893
Validator 4	5626.140496	5773.231405

Table 2: Data used for Average Block Processing

Table 2 shows the data used for analysis of average block processing, which were also used for creating the graph shown in figure 2.

6.2 CPU Utilization

The second experiment evaluated CPU resource usage by validators in both benign and DDoS traffic environments. The result shows a slight rise in CPU utilization during DDoS attack, which shows that while such kind of attack happens, there is an additional strain on system resources. The overall impact may vary based on the severity of the attack and the resilience of the system.

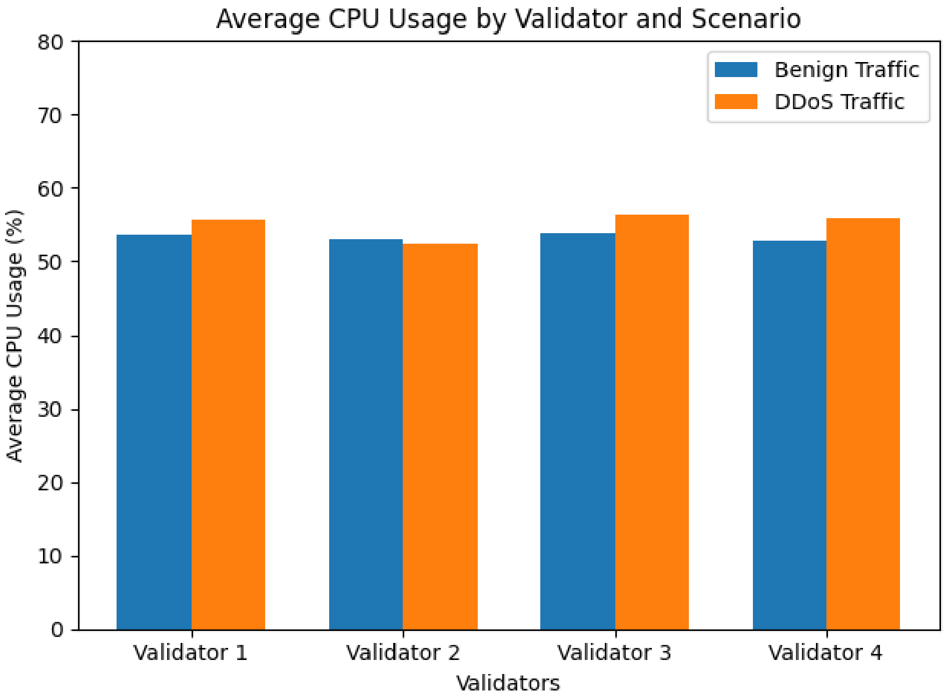


Figure 3: Comparison of Average CPU Usage between DDoS Traffic and Benign Traffic

The graph shown in figure 3 clearly illustrates that the average CPU usage of validators during the DDoS attack is changing gradually. Because there are a large number of transactions to handle and manage a bigger transaction pool is needed. While under benign traffic, the graph is relatively stable as compared to during a DDoS attack.

Validators	**CPU Usage of DDoS Traffic (%)**	**CPU Usage of Benign Traffic (%)**
Validator 1	55.727273	53.669421
Validator 2	52.462810	53.099174
Validator 3	56.429752	53.909091
Validator 4	55.925620	52.776860

Table 3: CPU Usage Comparison Between DDoS and Benign Traffic

The data mentioned in table 3 shows the CPU utilization of blockchain during normal traffic and traffic during DDoS attack.

6.3 Network Traffic Analysis

The third experiment focused on the comparative analysis of network traffic by analyzing ingress and egress rates under normal traffic, traffic after processing benign data and traffic after processing DDoS data. The results showed that there was a significant rise in ingress and egress during DDoS attacks. This proves that these attacks can saturate network bandwidth and validates the efficiency of network based detection methodologies.

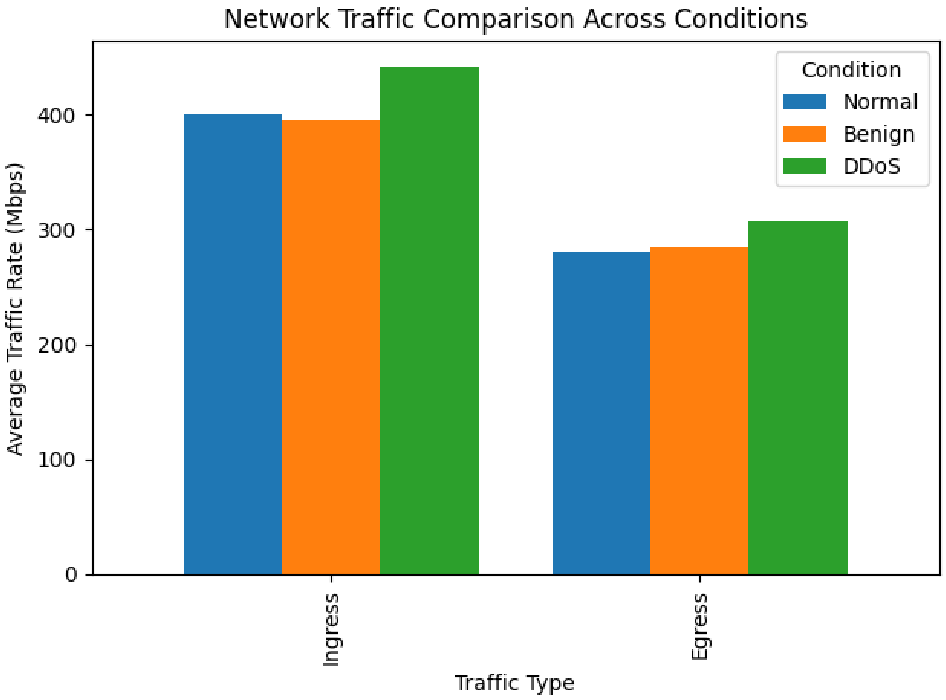


Figure 4: Network Traffic comparison in Normal traffic, DDoS Traffic and Benign Traffic

The graph shown in figure 4 illustrates that DDoS attack show a noticeable rise in the network traffic as compared to normal traffic, which leads to increased latency in transaction propagation and processing. While with benign traffic, the network traffic is predictable with lower latency as compared to a DDoS attack.

Network Traffic	**Ingress**	**Egress**
Normal	400.000000	280.00000
Benign	394.818095	284.70381
DDoS	441.561404	307.50000

Table 4: Network Traffic Analysis: Ingress and Egress Values

The data mentioned in table 4 shows ingress and egress network values of normal traffic, traffic after sending benign data and traffic after sending DDoS data manually.

6.4 Discussion

The analysis of this research has focused on the impact of Distributed Denial of Service (DDoS) attacks on blockchain networks. This analysis utilized experimental methods to demonstrate how blockchain technology can be used to enhance security and transparency against such attacks. The results from these experiments show that integrating blockchain technology with machine learning may be an effective way to fight against DDoS attacks. The findings show that the extended block processing time, as shown in figure 5, indicates the network is in struggle due to DDoS attacks, but also it shows the network can still work even with increased load on it.

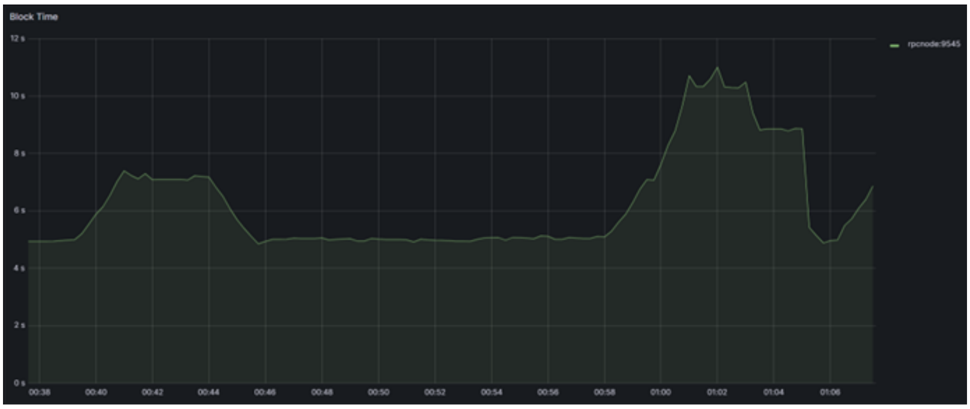


Figure 5: Block Processing Time during DDoS attack

Similarly, the increased CPU usage as shown in figure 6 illustrate that the system's response to detection and analysis of DDoS attack, which is important to maintain the network security and performance.

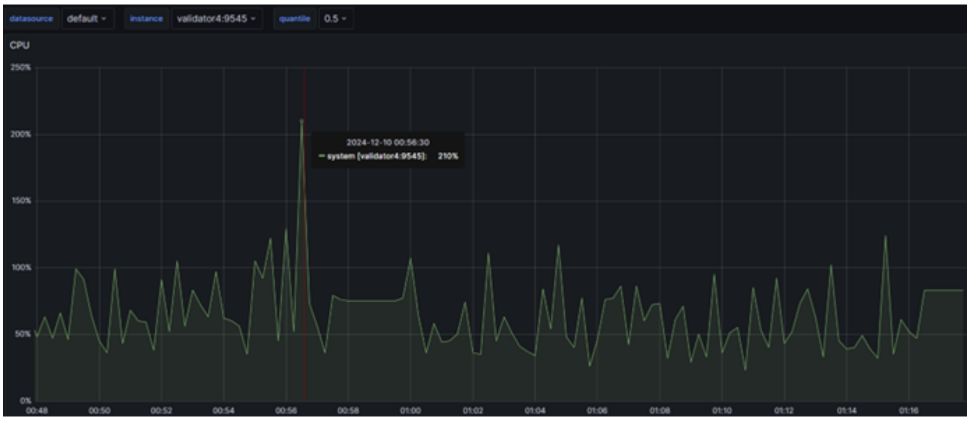
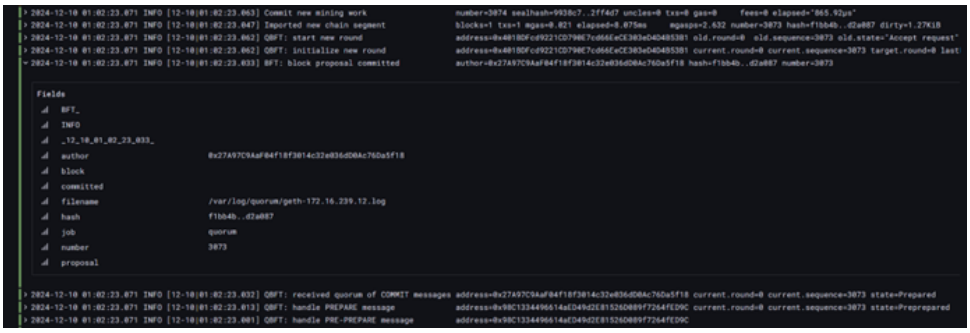

datasource default
instance validator4:9545
quantile 0.5

Figure 6: CPU Usage in percentage during DDoS attack

This aligns with the research done by Abdullah and Hussein (2024), which indicates that the resilience in blockchain framework under cyber threats.
The main goal of this research was to evaluate how the integration of blockchain technologies and machine learning could enhance the security and transparency in the detection and analysis of DDoS attacks within decentralized networks. The results of this research shows that the combination of blockchain technology and machine learning algorithms can effectively detect and analyze the DDoS attack. This integration improves the security by decentralizing the detection and eliminating single points of failure. It also enhances transparency by ensuring that all actions and decisions are stored in secure and tamper proof records. This research uses the Loki tool from Grafana to store the logs as shown in figure 7.

This aligns with the research done by Li et al. (2024), who observed that using blockchain in decentralized networks improves security features.



```
> 2024-12-10 01:02:23.071 INFO [12-10|01:02:23.063] Commit new mining work             number=3074 sealhash=9938c7..2ff4d7 uncles=0 txs=0 gas=0     fees=0 elapsed="865.92µs"
> 2024-12-10 01:02:23.071 INFO [12-10|01:02:23.047] Imported new chain segment         blocks=1 txs=1 mgas=0.021 elapsed=8.075ms     mgasps=2.632 number=3073 hash=f1bb4b..d2a087 dirty=1.27KiB
> 2024-12-10 01:02:23.071 INFO [12-10|01:02:23.062] QBFT: start new round              address=0x4018DFcd9221CD790E7cd66EeCE303eD4D485381 old.round=0  old.sequence=3073 old.state="Accept request"
> 2024-12-10 01:02:23.071 INFO [12-10|01:02:23.062] QBFT: initialize new round         address=0x4018DFcd9221CD790E7cd66EeCE303eD4D485381 current.round=0 current.sequence=3073 target.round=0 last
v 2024-12-10 01:02:23.071 INFO [12-10|01:02:23.033] BFT: block proposal committed      author=0x27A97C9AaF04f18f3014c32e036dD0Ac76Da5f18 hash=f1bb4b..d2a087 number=3073

    Fields
      BFT_
      INFO
      _12_10_01_02_23_033_
      author                        0x27A97C9AaF04f18f3014c32e036dD0Ac76Da5f18
      block
      committed
      filename                      /var/log/quorum/geth-172.16.239.12.log
      hash                          f1bb4b..d2a087
      job                           quorum
      number                        3073
      proposal

> 2024-12-10 01:02:23.071 INFO [12-10|01:02:23.032] QBFT: received quorum of COMMIT messages address=0x27A97C9AaF04f18f3014c32e036dD0Ac76Da5f18 current.round=0 current.sequence=3073 state=Prepared
> 2024-12-10 01:02:23.071 INFO [12-10|01:02:23.013] QBFT: handle PREPARE message        address=0x98C1334496614aED49d2E81526D089f7264fED9C current.round=0 current.sequence=3073 state=Preprepared
> 2024-12-10 01:02:23.071 INFO [12-10|01:02:23.001] QBFT: handle PRE-PREPARE message    address=0x98C1334496614aED49d2E81526D089f7264fED9C
```

Figure 7: Logs of Loki during DDoS attack

The decentralized nature of blockchain disperses data across multiple nodes, increases security, and makes it more challenging for attackers to find a single point of vulnerability for attack. The dispersion helps to prevent any single node from becoming point of failure during an attack, which improves the safety of the entire network.
Also, the transparency of the blockchain mechanism, which securely stores all transactions and supports the detection of possible threats, was significant in this research. Whenever the system detected a threat, it recorded that event on the blockchain, which provides transparent and auditable trail of the system's response to the DDoS attack. This helps to quickly respond to threats and allows one to review past events. This enhancement in the transparency of blockchain is supported by the research done by Xu et al. (2024). They have studied how blockchain supports the storage and handling of data securely.

7 Conclusion and Future Work

Conclusion:

The goal of this research was to enhance understanding of DDoS attacks impacting blockchain networks. This research analyzed how DDoS attacks affect the block processing duration, CPU utilization and overall network traffic behaviors on blockchain. This was done by examining the influence of DDoS as well as legitimate traffic on blockchain.

This research successfully met its objectives through comprehensive experiments that analyzed various performance metrics under both normal and attack scenarios. These experiments indicated that the blockchain network had become unstable during the DDoS attack. The analysis and results of these experiments are mentioned in the evaluation section of the research.

Still, this research has some limitations. The controlled testing setup used in the experiments might not fully capture the challenges and unexpected events that happen in real world blockchain operations and DDoS attacks. Also, not enough research has been done on the scalability of suggested detection strategies under various network conditions and with different levels of attack.

Future :

In the future, there is plenty of chance to keep working on this research. Future research could investigate the application of more advanced machine learning techniques like deep learning to enhance the precision and efficiency of DDoS detection systems.

Using these solutions in real-time blockchain environments could help to understand the effectiveness and scalability of them. Also, developing security measures that combines defenses at the bot application and network layers could provide protection against multi vector DDoS attacks.

As per the commercialization point of view, this research is really promising. Just like SOchain, the detection methodologies developed in this research could be marketed as specialized services for blockchain platforms to improve their security. Yeh et al. (2020). This could be really helpful for Blockchain as a Service (BaaS) providers searching to deliver enhanced value to their clients. Also, integrating these security advancements into current blockchain systems could create advantage for the businesses.

References

Abdullah, A. A. and Hussein, S. A. (2024). Detection and Mitigation Distribution Denial of Service Attack Based on Blockchain Concept., *Ingénierie des Systèmes d'Information* **29**(3): 1043–1049. Publisher: International Information & Engineering Technology Association (IIETA).
URL: *https://research.ebsco.com/linkprocessor/plink?id=409da195-020c-357c-bec0-739e7c050a9b*

Baliga, A., Subhod, I., Kamat, P. and Chatterjee, S. (2018). Performance Evaluation of the Quorum Blockchain Platform. arXiv:1809.03421.
URL: *http://arxiv.org/abs/1809.03421*

Correia, P. H. B., Marques, M. A., Simplicio, M. A., Ermlivitch, L., Miers, C. C. and Pillon, M. A. (2024). Comparative Analysis of Permissioned Blockchains: Cosmos, Hyperledger Fabric, Quorum, and XRPL, *2024 IEEE International Conference on Blockchain (Blockchain)*, pp. 464–469. ISSN: 2834-9946.
URL: *https://ieeexplore.ieee.org/document/10664236/*

Dong, S., Abbas, K., Li, M. and Kamruzzaman, J. (2023). Blockchain technology and application: an overview, *PeerJ Computer Science* **9**: e1705.

Ibrahim, R. F., Abu Al-Haija, Q. and Ahmad, A. (2022). DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology., *Sensors (14248220)* **22**(18): 6806–N.PAG. Publisher: MDPI.
URL: *https://research.ebsco.com/linkprocessor/plink?id=4f9fd49c-91bd-392a-b2e8-1dd16df7979f*

Jawahar, A., Pandurangan, K., C, V., R, V., R, A., K, B. and Vedhapuri, G. (2024). DDoS mitigation using blockchain and machine learning techniques, *Multimedia Tools and Applications* **83**: 1–14.

Li, C., Huo, D., Wang, Y., Wang, S., Deng, Y., Zhou, Q. and Wang, Y. (2024). A deep learning based detection scheme towards DDos Attack in permissioned blockchains, *2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 2644–2649. ISSN: 2768-1904.
URL: *https://ieeexplore.ieee.org/document/10580421/?arnumber=10580421*

Nasir, N. M., Hassan, S. and Mohd Zaini, K. (2024). Securing Permissioned Blockchain-Based Systems: An Analysis on the Significance of Consensus Mechanisms, *IEEE Access* **12**: 138211–138238. Conference Name: IEEE Access.
URL: *https://ieeexplore.ieee.org/document/10685412/?arnumber=10685412*

Pawar, P. P., Kumar, D., Ananthan, B., Pradeepa, A. and Selvi, A. (2024). An Efficient DDoS Attack Detection using Attention based Hybrid Model in Blockchain based SDN-IoT, *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)*, pp. 1–5.
URL: *https://ieeexplore.ieee.org/document/10574596/?arnumber=10574596*

Saveetha, D., Maragatham, G., Ponnusamy, V. and Zdravković, N. (2024). An Integrated Federated Machine Learning and Blockchain Framework With Optimal Miner Selection for Reliable DDOS Attack Detection, *IEEE Access* **12**: 127903–127915. Conference Name: IEEE Access.
URL: *https://ieeexplore.ieee.org/document/10555270/?arnumber=10555270*

Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S. and Gulzar, Y. (2021). Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight, *Symmetry* **13**(2): 227. Number: 2 Publisher: Multidisciplinary Digital Publishing Institute.
URL: *https://www.mdpi.com/2073-8994/13/2/227*

Xu, C., Jin, G., Lu, R., Zhu, L., Shen, X., Guan, Y. and Sharif, K. (2024). A Federated Learning Architecture for Blockchain DDoS Attacks Detection, *IEEE Transactions on Services Computing* **17**(5): 1911–1923. Conference Name: IEEE Transactions on Services Computing.
URL: *https://ieeexplore.ieee.org/document/10663969/*

Yeh, L.-Y., Lu, P. J., Huang, S.-H. and Huang, J.-L. (2020). SOChain: A Privacy-Preserving DDoS Data Exchange Service Over SOC Consortium Blockchain, *IEEE Transactions on Engineering Management* **67**(4): 1487–1500. Conference Name: IEEE Transactions on Engineering Management.
URL: *https://ieeexplore.ieee.org/document/9040569/?arnumber=9040569*