Token Based Approach for Resource Management in IoT Edge Networks

Yernur Aubakirov, Yersultan Tursyn, Yerassyl Maratov, Meiirkhan Sakenuly, Nukhan Kadirov
4th Year Computer Science Students
Nazarbayev University
Astana, Kazakhstan
{yernur.aubakirov, yersultan.tursyn, yerassyl.maratov, meiirkhan.sakenuly, nukhan.kadirov}@nu.edu.kz

Professor Latif Zohaib
Mentor, Department of Computer Science
Nazarbayev University
Astana, Kazakhstan
latif.zohaib@nu.edu.kz

***Abstract*—The growth of the Internet of Things has created challenges in managing network resources and preventing malicious users from exploiting the system. Traditional networking approaches lack scalability and the flexibility to adapt to dynamic resource demands. This project presents an approach to managing IoT edge networks using SDN (Floodlight), simulated blockchain token systems (Ganache), and Dockerized IoT nodes. We successfully implemented a system that filters abnormal requests, incentivizes computational fairness, and visualizes token balance over time. Results show effective request management and traceable resource consumption using blockchain logic.**

***Index Terms*—IoT, Resource Management, Token-Based Systems, Software-Defined Networking (SDN), Blockchain, Edge Computing, Network Security, Smart Contracts, Malicious User Prevention**

I. Introduction

The increasing adoption of the Internet of Things (IoT) has been received with great enthusiasm because of the innovation that it brings to different industries. But this kind of growth also brings about major problems. One of them is the IoT device constraints, mainly regarding storage and processing power. Moreover, conventional networking approaches that rely on the implementation of headers, hardware infrastructure, and distributed control systems aggravate the picture by resulting in starchy networks that are a nightmare to manage, let alone scale up.

Edge Computing (EC) has come up as a viable solution to addressing these challenges. EC leverages many edge devices so that they can operate in unison to meet user demands in a more optimized manner. However, there are challenges when it comes to implementing EC, these include identifying the right places where task offloading should occur and guaranteeing that data flows and workloads are fairly distributed across edge devices. Added to this, malicious devices can take place in this technology by consuming and requesting a lot of data (power). All these challenges are made worse by the fact that the use of IoT resources is constantly increasing due to the increasing number of connected IoT devices.

One possible solution to address such challenges is the use of a combined System Software Defined Networking (SDN) and Blockchain (BC) strategy. SDN offers controllership and network visualisation in real-time and separates the data plane from the controller plane. Separation improves decision making, flow control and efficient usage of data flows by providing a global view over the network and application of general rules as needed. At the same time, the idea of intelligent smart contacts is introduced by Blockchain technology, providing the safe and automated control of IoT devices through token distribution. The general idea is that each IoT device will get a certain amount of tokens and each request for the computing resources made by the device will consume some amount of tokens. Thus token transactions can serve as a guarantee that even though some malicious users appear they can not lock the resources by sending an enormous amount of requests.

This project focuses on developing a token-based resource management system for IoT edge networks, leveraging SDN and BC technologies to manage network resources efficiently and securely. The system ensures that resources are allocated fairly across IoT devices using a token economy while preventing malicious activities. The main objectives of the project include:

- Designing a scalable token-based resource management system to allocate resources fairly among IoT devices in an edge network.
- Integrating SDN technology for centralized network control, enabling dynamic resource allocation based on real-time network conditions.
- Utilizing blockchain to track and verify resource usage, ensuring transparency, security, and immutability of transactions.
- Implementing a smart contract system for automatic enforcement of resource allocation rules and to prevent unauthorized access or misuse of resources.
- Optimizing network path selection to minimize latency

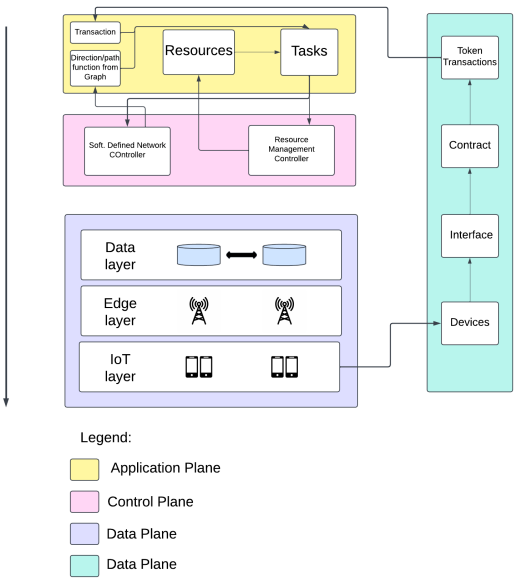

Fig. 1. SD system design and layers

and improve task completion times for IoT devices.

- Ensuring system robustness by testing it under various use cases, including scalability testing, malicious flooding prevention, and token security validation.
- Providing real-time monitoring through a user-friendly interface that logs token balances, request flows, and task execution metrics.
- Validating the system through performance benchmarks, demonstrating its ability to efficiently handle network tasks while maintaining fairness and security.

As shown in figure 1, using SDN technology for network management and Blockchain technology for services (token) distribution, this approach might deliver essential efficiencies and density increase to IoT and EC markets. Combined, these technologies contribute a comprehensive approach to solving the emerging problems in IoT resource management and network configurations.

II. Background and Related Work

The rapid adoption of the IoT has led to exponential growth in connected devices, necessitating efficient resource management solutions to address computational and storage limitations. Edge Computing has emerged as a promising paradigm to mitigate these issues by enabling resource sharing among edge devices. However, this paradigm presents challenges in terms of task offloading, flow scheduling, and load balancing. Traditional cloud-based paradigms, as powerful as they are, are increasingly unable to deliver the low latency and responsiveness required of current IoT applications. Their reliance on centralized infrastructure lead to bottlenecks, delayed processing, and security breaches, particularly where sensitive data is to be processed across distances to distant data centers. In response to these limitations, edge computing has gained traction owing to its ability to shift processing closer to end devices. Such a shift in architecture helps in reducing latency and traffic in core networks. But while edge computing improves some of the performance issues, it introduces new coordination, fairness, and security challenges in a decentralized network of nodes.

Managing resources in such an environment requires intelligent orchestration of task distribution, nuanced management of device behaviors, and robust security to make sure the system is not being abused. Edge networks, which are heterogeneous devices of varying capability and ownership, are especially vulnerable to selfish or malicious users who may attempt to manipulate the use of resources or disrupt services. Without tools to monitor, enforce, and promote proper use of shared computation resources, edge environments can be inefficient and unstable. In addition, the mobile nature of IoT networks, with devices frequently changing location or entering and exiting, complicates keeping performance fair and consistent.

A. Challenges in IoT Resource Management

IoT devices often suffer from limited computational and storage resources. Traditional cloud computing approaches fail to meet the low-latency and scalability requirements due to the physical distance between devices and centralized cloud servers. Emerging edge computing technologies aim to address these issues by bringing computational resources closer to IoT devices, thereby reducing latency and enhancing system responsiveness. Nevertheless, the integration of edge computing introduces its own challenges, including efficient resource allocation and security.

B. Existing Solutions and Limitations

Resource management in IoT edge networks must balance limited device resources, dynamic workloads, and security requirements. A promising approach is to integrate SDN and blockchain to orchestrate edge resources and enforce trust through token-based incentives. One early example is the EdgeChain framework, which links IoT devices to edge cloud resources via a permissioned blockchain with an internal token currency system. Smart contracts in EdgeChain automatically enforce resource access policies, and its prototype showed that a credit-based ledger can improve resource utilization while preserving security constraints (i.e., only trusted devices with sufficient tokens consume edge resources). This demonstrated the feasibility of decentralized resource governance at the network edge, a concept our work builds upon by likewise employing tokens for accountability and fair resource sharing [6].

Recent research has extended such blockchain-driven resource management with SDN's global control to optimize network performance. For instance, SDBlockEdge combines an SDN controller's holistic network view with blockchain smart contracts to coordinate multi-hop computation offloading in collaborative edge computing. In this scheme, IoT tasks are offloaded along paths selected by the SDN controller, and edge resources are allocated in exchange for tokens recorded on a blockchain. The token mechanism, enforced by smart

contracts, incentivizes honest behavior and prevents any single IoT node from abusing shared resources. Experiments showed that this integration of SDN and blockchain can reduce task completion time by balancing loads across edge servers while logging resource usage immutably for accountability [1]. Similarly, the SmartBlock-SDN framework uses an SDN infrastructure together with a blockchain ledger to securely manage IoT resources. In SmartBlock-SDN, the controller optimizes network routes and bandwidth allocation, and the blockchain provides a tamper-proof record of resource transactions and node reputations. This combination was shown to improve energy efficiency and throughput in IoT networks under heavy loads by dynamically selecting optimal edge nodes (e.g., cluster heads) and ensuring trust among participants via smart-contract automation [5]. Both SDBlockEdge and SmartBlock-SDN highlight the benefits of unifying SDN's programmability with blockchain's decentralized trust: the former focuses on multi-hop task offloading, while the latter emphasizes overall resource optimization and security. These approaches address core issues in our project (secure offloading and fair resource allocation) by using token-based accounting to coordinate edge nodes, but they do not yet incorporate advanced intelligence for decision-making.

In addition, Kherraf et. al. have explored various methods for optimizing edge resource provisioning in IoT networks, particularly in environments where workloads are heterogeneous and vary dynamically. One significant approach involves leveraging SDN alongside cloud and edge computing, as seen in the work by Kherraf et al., who propose a mixed-integer programming formulation for MEC resource provisioning. This model minimizes latency and computational costs by efficiently placing edge servers and assigning tasks based on workload requirements, showing that edge provisioning can significantly improve task execution times in heterogeneous IoT environments [12]. Similarly, Hussain et al. discuss how machine learning techniques are being used for dynamic resource management in IoT networks. They highlight the use of reinforcement learning (RL) for spectrum management and deep learning (DL) for optimizing resource allocation, which can enhance real-time decision-making in congested or variable environments [13]. These approaches are particularly relevant to our project, as they show how learning algorithms can optimize dynamic resource allocation at the edge.

In industrial IoT (IIoT) applications, the need for efficient resource orchestration is especially critical. Okwuibe et al. present a software-defined resource management (SDRM) model that applies constraint satisfaction problem (CSP) formulations to determine the optimal resource allocation for IIoT tasks, ensuring that service level agreements (SLAs) are met while minimizing costs. This framework uses SDN for centralized resource management, dynamically adjusting allocations based on application requirements in real-time [15]. Similarly, Alam et al. propose a programmable SDN-based architecture for IIoT that facilitates the dynamic reconfiguration of edge services. Their approach optimizes task scheduling and resource distribution to meet diverse industrial needs, demonstrating the ability of SDN to adapt to the varying demands of IoT devices across the industrial spectrum [14]. These studies contribute to the growing body of work that explores SDN's role in dynamically orchestrating resources in complex, heterogeneous environments, supporting the need for robust, flexible solutions in industrial and non-industrial edge networks.

To further encourage cooperation among distributed edge nodes, researchers have proposed incentive-driven resource sharing schemes. A representative study introduces a blockchain-based auction mechanism to improve collaborative edge computing efficiency under different owners' domains. In this approach, each edge server bids via a Vickrey-Clarke-Groves auction for tasks, and a blockchain maintains a transparent ledger of contributions and rewards. By combining a game-theoretic incentive (payment for handling others' tasks) with an immutable task log, the system achieves better load balancing across trust boundaries. The blockchain ensures that edge servers are compensated with tokens according to the truthful reporting of their available capacity and completed workloads, which in turn motivates them to assist other nodes' IoT tasks [7]. In a related vein, a decentralized IoT resource monitoring and scheduling framework uses blockchain to harness the idle computing power of IoT devices at the network edge. Here, the blockchain's smart contracts verify device computing capacity and track task execution results, enabling idle devices to credibly contribute to edge workloads. This framework addresses the problem of underutilized IoT hardware by forming a secure resource pool: devices "earn" tokens or reputation for lending compute power, and the ledger audits each task's outcome to discourage malicious results. Simulation of a distributed machine-learning task demonstrated that this blockchain-based scheduling can dramatically improve task throughput by tapping unused resources without requiring a central coordinator [8]. These incentive-oriented solutions are closely aligned with our problem context, as they show how token economies and transparent ledgers can engender cooperation and prevent free-riding in edge networks. Our work similarly aims to prevent resource misuse by malicious nodes, but with a more holistic integration of network management and incentive policies.

Beyond blockchain-based trust enforcement and AI-driven coordination, formal optimization techniques have been widely used to tackle resource scheduling in large-scale IoT ecosystems. One significant contribution comes from work on IoT-based smart cities, where researchers proposed a suite of edge resource allocation algorithms designed to minimize average service response time under constrained capacities and diverse application demands [11]. The study introduces both exhaustive and heuristic methods—EOERA and CHERA—for distributing limited edge server resources across competing applications with varying latency and computational requirements. These approaches consider queueing delays, transmission latency, and cloud fallback penalties to determine optimal request routing and server assignments. While the framework does not include SDN or blockchain for control and enforce-

ment, it offers a well-structured model for prioritizing edge workloads based on service profiles and network topology. Such formal methods complement decentralized solutions by helping to inform policy decisions (e.g., where to assign tokens or when to offload to the cloud), and highlight the importance of integrating fairness-aware scheduling in token-based SDN-blockchain architectures.

Another line of relevant research uses artificial intelligence at the edge to improve resource allocation decisions. Rather than relying solely on predefined rules, these works apply machine learning to dynamically manage IoT workloads. For example, a recent SDN-based federated learning (FL) approach leverages distributed edge intelligence to allocate resources efficiently. The system trains ML models across IoT devices (using FL to keep data local) and uses the SDN controller to collect learning updates and coordinate network resources accordingly. This approach addresses issues like caching and load prediction by learning usage patterns from devices, and the SDN orchestrator then proactively adjusts resource provisioning (e.g., routing, bandwidth) based on the learned models. The result is an intelligent edge network that improves QoS (e.g., lower latency and congestion) without violating user privacy by sending raw data to the cloud [2]. While this FL-based solution does not employ blockchain, it introduces an intelligent automation dimension that complements the security and trust mechanisms of token-based frameworks. Another study focuses on deep reinforcement learning (DRL) for service function chain orchestration in cloud-edge environments. It formulates the placement of virtual network functions (VNFs) for IoT services as a sequential decision problem and trains a DRL agent to deploy and route SFCs optimally under latency and reliability constraints. Notably, this DRL-driven orchestration (augmented by a trust module) learns to place critical IoT services on reliable edge nodes or cloud servers to maximize performance while avoiding untrusted resources. The proposed system, tested in an IoT testbed, reduced service latency and automatically adapted to network changes, illustrating how AI can handle the complexity of edge resource management policies [4]. These intelligent control methods are relevant to our project as they could enhance how the token-based SDN-blockchain framework makes decisions (e.g., which node should get tokens for a task) — potentially, our system can integrate learning components to adapt token pricing or resource scheduling in real time.

Some works have gone further to merge incentive models with learning. Wang et al. [9] introduce an incentive-aware federated deep reinforcement learning scheme for joint edge caching and computation offloading in IoT. In their design, multiple edge nodes collaboratively train a DRL agent (via federated learning) to minimize overall task latency and cost, while a blockchain-based smart contract rewards nodes that participate actively in the training and offloading process. By making the training contribution of each node transparent on a ledger, the system encourages nodes to cooperate (e.g., share bandwidth for caching or execute others' tasks) in exchange for token rewards. This leads to improved caching hit rates and lower execution costs compared to non-incentivized baselines. Another recent work proposes a merit-based multi-task scheduling algorithm for 6G edge networks that integrates blockchain and federated learning [10]. It considers heterogeneous IoT tasks with different priorities and deadlines, and uses a blockchain to securely coordinate FL model updates and access control. The scheduling algorithm allocates edge server resources to tasks based on a "merit" score that combines task urgency, the requesting device's trust score, and its past contributions (learned via FL). The blockchain records these metrics and the scheduling decisions, ensuring transparency. This approach achieved about 45% reduction in task completion time and 53% cost savings by intelligently prioritizing resource allocation while using blockchain for data integrity. These hybrid solutions illustrate the trend of combining AI-driven optimization with blockchain incentives in edge computing. They relate to our work by suggesting that beyond basic token accounting, incorporating learning (to predict demand or detect cheating) could further enhance a token-based resource management framework.

Finally, beyond incentive and learning-based approaches, researchers have tackled IoT edge resource management through rigorous optimization and virtualization techniques. For example, Pham and Nguyen [3] formulate a multi-layer optimization model for NFV-enabled IoT edge clouds. Their model jointly optimizes IoT gateway deployment, multi-hop routing in the device layer, and service function placement in edge and cloud servers. By capturing these decisions in a unified cost function (with terms for latency, deployment cost, and resource usage), they derive an optimal allocation of resources for a given IoT application demand. Because the exact optimization is NP-hard, they also develop approximation algorithms that can handle large-scale scenarios with many IoT nodes and limited edge servers. The evaluation shows that their approach closely approximates the optimal solution while drastically reducing computation time, and it provides insights such as: placing latency-critical functions at the edge while offloading less sensitive tasks to the cloud yields the best cost-performance tradeoff. This kind of deterministic optimization complements our token-based approach by offering theoretical bounds and algorithms for resource placement; in practice, our blockchain/SDN framework could incorporate such algorithms in the SDN controller to decide how to allocate resources to token holders most efficiently.

In summary, prior works have made important strides in IoT edge resource management through decentralized trust mechanisms, incentive allocation, intelligent orchestration, and formal optimization. Blockchain-based frameworks with token economies (e.g., EdgeChain, SDBlockEdge) address the security and fairness issues by decentralizing control and accountability. SDN-based solutions provide the needed agility to configure network paths and allocate bandwidth on the fly. Meanwhile, AI-driven approaches (FL and DRL) can automate complex decisions and adapt to workload patterns, and NFV-oriented optimizations ensure that the infrastructure is utilized optimally. However, no single solution yet provides a

holistic integration of network programmability, decentralized trust, and adaptive intelligence. For instance, most blockchain-focused schemes do not leverage learning for predictive optimization, and many learning-based or optimization works assume a trusted environment. Our work aims to fill this gap by combining SDN, blockchain, and a token-based reward system into one unified framework. By doing so, we ensure real-time resource allocation decisions with the SDN controller, secure and transparent enforcement of those decisions via blockchain smart contracts, and an incentive layer (tokens) to encourage cooperative behavior among IoT devices. The proposed approach builds on the ideas reviewed above and integrates them to provide a more comprehensive solution to resource management in IoT edge networks.

TABLE I
COMPARISON OF RELATED WORKS

Related Work	Malicious Filtering	Token-Based Access	Smart Contracts	SDN Integration	Dockerization	Real-Time Visualization
EdgeChain	✗	✓	✓	✗	✗	✗
SDBlock-Edge	✓	✓	✓	✓	✗	✗
Smart Block-SDN	✗	✓	✓	✓	✗	✓
Auction Mechanism	✓	✓	✓	✓	✗	✗
Idle IoT Scheduling	✓	✓	✓	✓	✗	✗
Zhao et al. (Smart Cities)	✗	✗	✗	✗	✗	✗
FL with SDN	✗	✗	✗	✓	✗	✓
DRL for SFC	✓	✗	✓	✓	✗	✓
Federated Deep RL	✓	✓	✓	✓	✗	✗
NFV Optimization	✗	✗	✗	✓	✓	✗
SDRM for IIoT	✗	✗	✗	✓	✓	✗
Our Solution	✓	✓	✓	✓	✓	✓

C. Proposed Contributions

This work introduces a novel framework combining SDN and BC to address the aforementioned challenges. By utilizing SDN's global network visibility and BC's secure smart contract mechanisms, the proposed approach ensures optimal task offloading, flow scheduling, and resource management. Additionally, the integration of a token-based system facilitates accountability and prevents resource misuse by malicious IoT devices. This framework aims to fill the gaps in the existing literature by providing a holistic solution to IoT resource management.

III. PROJECT DESCRIPTION

A. System Features

The system incorporates several key features. Firstly, it utilizes Token-Based Resource Allocation, where each IoT device is initially given a specific quantity of tokens. These tokens serve as a currency for requesting network services and are paid to the controller upon use. The controller periodically redistributes these tokens among the IoT devices after a set time frame. Secondly, Blockchain-Enabled Security is integral; the system employs blockchain technology to securely record all token transactions. Smart contracts are used to automate control mechanisms and enforce operational rules without intermediaries, guaranteeing transparency and creating tamper-proof records of every transaction. Lastly, the system features Dynamic Network Management achieved through Software-Defined Networking, which effectively separates the data plane from the control plane. This allows for centralized network management and visualization of the network topology via the controller, which also enhances flow management by applying rules globally across the network.

B. Requirements and Functionalities

The project adheres to specific functional and non-functional requirements. Functionally, the system must manage Token Allocation and Management; upon network initialization, every IoT device receives an initial token balance. These tokens are automatically deducted when resources are accessed and can be replenished according to predefined conditions. Secure Resource Requests are also required, meaning all requests for resources must include authentication credentials, and token balances must be checked before granting access.

Non-functionally, security is paramount. Communication channels should be encrypted to preserve data integrity. IoT device authentication needs to be robust to prevent malicious activities, and the system requires protection against common threats like DDoS, spoofing, and replay attacks. Scalability is another critical non-functional requirement; the system must be capable of handling a growing number of devices without performance degradation, and the architecture needs to support the seamless onboarding of new nodes.

C. Design

The system's design encompasses its architecture and operational workflow. The System Architecture involves IoT Devices, each starting with an initial token balance used for resource access. These devices send resource requests that include unique authentication data, such as their IP address and identifier. Edge Computing Nodes provide the computational services requested by the IoT devices. These nodes interface with both the SDN controller and the blockchain network to validate requests and log the execution of tasks based on token payments.

The operational Workflow begins with Initialization, during which token balances are assigned to devices. The network itself is emulated using Mininet, employing a Floodlight

controller to achieve centralized control and provide visibility into the network topology. In the Resource Request Process, IoT devices submit their requests containing embedded authentication details. The controller verifies the availability of the requested resource and, upon approval, deducts the necessary tokens from the balance of the requesting device.

IV. Project Implementation

The project focused on developing a token-based resource management system for IoT edge networks, incorporating Software-Defined Networking and blockchain technologies. The primary objective was to design an efficient and scalable system for managing resources in IoT edge environments, ensuring fairness and security in task allocation through token-based mechanisms. The system utilizes the Floodlight SDN controller, Mininet-WiFi simulation environment, Docker containers, and the Ganache Ethereum blockchain to simulate real-world network operations.

The system was implemented in stages, with the first phase involving the setup of the underlying infrastructure. The Mininet-WiFi topology was integrated with Docker-hosted IoT devices, providing a scalable simulation environment for testing and validation. A custom network topology combining WiFi access points, Docker containers, and switches was designed, enabling flexible network configurations and efficient resource management. To facilitate token management and incentivize fair usage, an Ethereum-based token system was developed using Ganache to simulate task payments and ensure resource fairness through smart contracts.

A significant accomplishment of the project was the implementation of a request filtering mechanism through tokenization. This mechanism allowed for the identification and blocking of abnormal or excessive resource requests, ensuring that only legitimate users had access to resources. Additionally, the system was equipped with visualization and logging capabilities, enabling real-time tracking of token balances, request flows, and task execution metrics, which provided insight into the efficiency and fairness of the resource allocation process.

During the semester, a key focus was on optimizing the system to improve its efficiency and scalability. The network path optimization was a critical area of development. By fetching real-time topology data, the system was able to dynamically calculate the shortest paths, reducing the time it takes for tasks to be offloaded and ensuring optimal utilization of available resources. In conjunction with the optimization efforts, extensive testing was conducted to ensure the system's robustness and functionality under various scenarios. These tests included functional testing of individual modules (e.g., SDN controller, blockchain smart contracts), scalability testing to evaluate performance under high traffic, and malicious flooding tests to simulate attacks and assess the system's ability to prevent unauthorized task submissions. Additionally, token security tests were implemented to validate the robustness of the token-based access control system, while blockchain spamming tests ensured that invalid transactions did not compromise the performance of the system.

By the end of the project, the core objectives had been successfully met, with a fully functional and tested system that incorporated both optimization and security features. The system was capable of dynamically managing resource allocation, ensuring fairness through blockchain-based token transactions, and protecting against malicious actions by filtering abnormal requests.

This implementation provides a solid foundation for further development and real-world deployment of the token-based resource management system in IoT edge networks, demonstrating its potential for practical applications in edge computing environments.

V. Future Work and Improvements

While the core architecture of the project has been implemented and tested, several improvements could further enhance the system. One of the primary improvements would be real-world deployment. Deploying the system on actual IoT hardware, such as Raspberry Pi or edge gateways, would provide an opportunity to assess performance in non-simulated environments. Another potential enhancement is scalability. Replacing Ganache with a full Ethereum testnet or exploring more scalable blockchain platforms, such as Polygon or Avalanche, could improve the overall system's ability to handle larger networks.

Additionally, integrating intelligent task schedulers that prioritize tasks based on urgency, energy constraints, or predicted outcomes could significantly enhance the system's efficiency. A user interface is another area of future development. Developing a live dashboard for real-time monitoring of requests, balances, and task statistics would improve user experience and provide more interactive management tools. Lastly, robust load handling techniques, such as introducing load balancing and asynchronous task queues, could improve the system's ability to manage high volumes of concurrent IoT requests, ensuring that the system remains efficient even under heavy workloads.

These directions provide a pathway for future researchers and developers to build upon the system for practical IoT applications. We believe addressing these areas will make the system deployable in production-grade edge infrastructures.

VI. Ethical and Legal Considerations

The integration of SDN and Blockchain technologies in IoT resource management introduces several ethical and legal considerations that must be addressed to ensure responsible deployment.

A. Data Privacy and Security

The system's reliance on token-based transactions and blockchain for resource allocation necessitates the collection and processing of device-specific data. To protect user privacy, all data is anonymized, and robust encryption protocols are implemented to secure communications between IoT devices and the controller. Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), is maintained to uphold user rights and data confidentiality.

B. Fairness and Non-Discrimination

The token allocation mechanism is designed to ensure equitable access to network resources among IoT devices. By implementing transparent and unbiased algorithms, the system prevents any form of discrimination or preferential treatment, thereby promoting fairness in resource distribution.

C. Transparency and Accountability

Utilizing blockchain technology provides an immutable and transparent ledger of all token transactions and resource allocations. This transparency fosters accountability, allowing for auditing and verification of system operations to detect and address any anomalies or misuse.

D. Legal Compliance

The deployment of this system is conducted in adherence to applicable laws and regulations governing data usage, network security, and digital transactions. Continuous monitoring of the legal landscape ensures that the system remains compliant with evolving legal standards and industry best practices. To avoid legal issues with intellectual property, the team relied on open-source tools and frameworks such as Ganache, Containernet, and Mininet for the development and implementation of networks.

E. Sustainability and Social Responsibility

In the era of constant technological advances, with the recent popularity of Cloud services, such as Amazon Web Services (AWS) and Google Cloud, demand for digital resource management systems is at its highest. This project addresses sustainability by enabling more effective resource management within IoT edge networks using a blockchain-based approach. In real-world applications, such as smart cities, this system can help optimize urban infrastructure by dynamically adjusting resource allocation to meet demand during peak times while avoiding bottlenecks. This adaptability enhances system reliability while advancing societal goals by fostering smarter, more resilient technologies to meet the demands of growing urban populations. By providing fair access and preventing misuse, the project reflects a commitment to social responsibility and supports the development of reliable and sustainable IoT ecosystems.

F. Ethical Design and Development

Throughout the development process, ethical considerations are integrated into system design decisions. This includes conducting thorough risk assessments, engaging with stakeholders to understand potential ethical implications, and implementing measures to mitigate identified risks. By prioritizing ethical principles, the system aims to contribute positively to the IoT ecosystem while safeguarding user interests.

By addressing these ethical and legal considerations, the system aspires to set a standard for responsible innovation in IoT resource management, balancing technological advancement with societal values and legal obligations.

VII. Results

To evaluate the performance and functionality of our token-based resource management system in an IoT edge network, we conducted several simulation scenarios. This section presents visualizations and insights from our experiments.

A. Request Counter Comparison

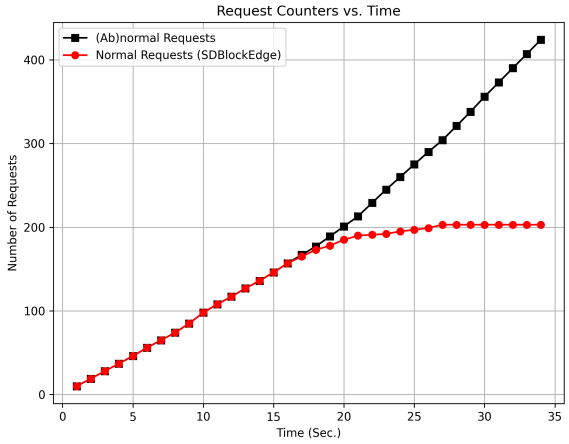

Fig. 2. Request Counters vs. Time: Comparing total requests versus normal requests under SDBlockEdge.

Figure 2 shows the number of total vs. filtered (normal) requests over time. The SDBlockEdge mechanism effectively reduces abnormal requests after the 18th second, illustrating its efficiency in mitigating spammy or malicious traffic in edge networks.

B. Docker Host Balances Over Time

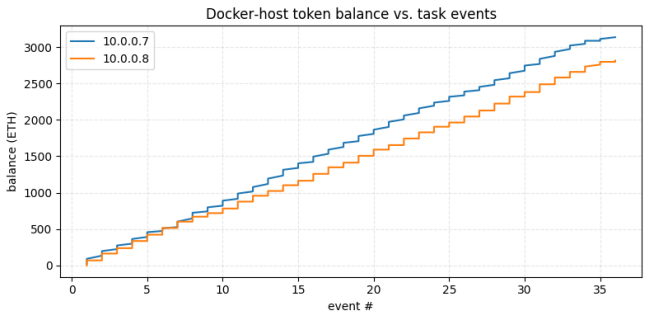

Fig. 3. Docker-host token balance changes over sequential task events.

Figure 3 compares token balances between two Docker hosts. The consistently increasing balance indicates successful task execution and token accrual via fair resource utilization.

C. Network Topology Visualization

Figure 4 depicts our SDN-based network topology. It combines physical and virtual elements (Wi-Fi APs, Docker hosts, Mininet switches), providing a flexible environment for edge computing and traffic management.

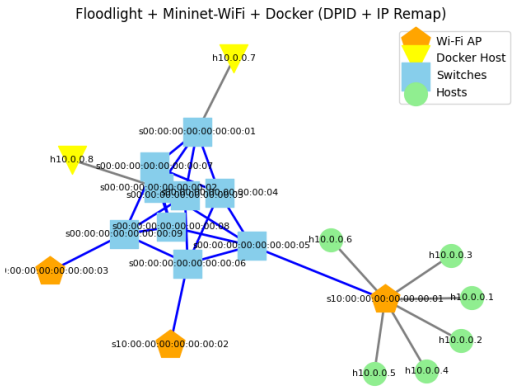

Fig. 4. Custom Network Topology: Integration of WiFi APs, Docker Hosts, Switches, and IoT Nodes.

D. IoT Device Token Expenditure

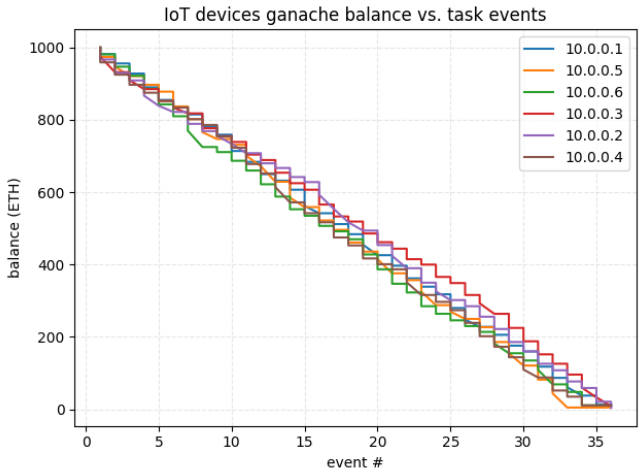

Fig. 5. IoT devices' token balance reduction with increasing task load.

In Figure 5, we observe token balances decreasing as IoT nodes complete tasks. This validates our Ethereum-based token system, where computational effort is tied to resource usage and incentivization.

VIII. Conclusion

This project successfully demonstrated the integration of Software-Defined Networking, blockchain, and edge computing principles to address the complex challenges of resource management in IoT environments. By combining SDN's global network visibility with the security and accountability features of blockchain, we developed a robust, scalable system for managing tasks and resources across edge devices. The system leverages a token-based incentive mechanism that ensures fairness in resource allocation while preventing malicious activities such as excessive resource requests.

Throughout the project, we implemented and tested a variety of technologies, including the Floodlight SDN controller, Mininet-WiFi, and Ganache Ethereum blockchain. The integration of these components allowed us to simulate realistic network topologies and evaluate the system's performance in managing tasks, ensuring that each IoT device could fairly access resources based on a token-based economy. This approach was validated through multiple tests, such as functional testing, scalability testing, and malicious flooding tests, all of which showed the system's capability to handle high traffic, maintain security, and prevent misuse.

A key achievement was the successful implementation of a request filtering mechanism, using tokenization to block excessive or unauthorized requests. This feature ensured that resources were only allocated to legitimate tasks, thereby preventing denial-of-service attacks and improving overall system reliability. Additionally, real-time logging and visualization capabilities were incorporated to track token balances and request flows, which provided transparency and traceability of resource usage.

One of the most significant contributions of this work is the optimization of network path selection, which was achieved by dynamically calculating the shortest paths based on real-time topology data. This optimization greatly improved the efficiency of task offloading, reducing latency and enhancing resource utilization. Extensive testing confirmed the effectiveness of these optimizations and highlighted the system's ability to adapt to varying network conditions and traffic loads.

The system's robustness was further demonstrated through security tests, which validated the token-based access control system and tested the resilience of the blockchain against spamming attempts. These tests showed that the system could maintain low latency while ensuring the integrity and authenticity of transactions, which is crucial for maintaining trust in decentralized networks.

As a result of these efforts, the project met its primary objectives of ensuring fair resource allocation, preventing malicious behavior, and providing scalability in IoT edge networks. The project's contributions offer a promising foundation for real-world deployment in edge computing environments, and the combination of SDN and blockchain provides a powerful tool for managing dynamic and heterogeneous networks efficiently.

Looking forward, there are several avenues for further improvement. Future work could explore the integration of AI to enhance decision-making, further optimization of network management algorithms, and the exploration of larger-scale deployments. The framework could also benefit from incorporating advanced machine learning techniques to predict resource usage patterns and improve task scheduling decisions in real-time. Moreover, deploying the system in a real-world environment would provide valuable insights into its performance outside of simulated conditions, leading to further refinements and scalability improvements.

In conclusion, this project has laid the groundwork for an innovative approach to IoT resource management, combining SDN, blockchain, and token-based incentives to create a

system that is both efficient and secure. The findings and technologies developed in this project offer significant contributions to the field of edge computing and IoT networks, with potential applications in smart cities, industrial IoT, and other resource-constrained environments.

REFERENCES

[1] Z. Latif, C. Lee, K. Sharif, and S. Helal, "SDBlockEdge: SDN-Blockchain Enabled Multihop Task Offloading in Collaborative Edge Computing," *IEEE Sensors Journal*, vol. 22, no. 15, pp. 15537-15547, Aug. 2022.

[2] V. Balasubramanian, M. Aloqaily, M. Reisslein, and A. Scaglione, "Intelligent Resource Management at the Edge for Ubiquitous IoT: An SDN-Based Federated Learning Approach," *IEEE Network*, vol. 35, no. 5, pp. 114–121, Sep./Oct. 2021.

[3] T. M. Pham and T. L. Nguyen, "Optimization of Resource Management for NFV-Enabled IoT Systems in Edge Cloud Computing," *IEEE Access*, vol. 8, pp. 178217–178233, Oct. 2020.

[4] S. Guo, Y. Dai, S. Xu, X. Qiu, and F. Qi, "Trusted Cloud-Edge Network Resource Management: DRL-Driven Service Function Chain Orchestration for IoT," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6010–6022, Jul. 2020.

[5] A. Rahman, M. J. Islam, A. Montieri, M.K. Nasir, N. Kumar, and A. Y. Zomaya, "SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT," *IEEE Access*, vol. 9, pp. 28361–28378, Feb. 2021.

[6] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: An Edge–IoT Framework and Prototype Based on Blockchain and Smart Contracts," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 4719–4732, 2019.

[7] Q. Gao, X. Wang, L. Zhao, et al., "Blockchain-based Collaborative Edge Computing: Efficiency, Incentive and Trust," Journal of Cloud Computing, vol. 12, article 72, 2023.

[8] D. Li, R. Chen, Q. Wan, Z. Guan, Y. Sun, Q. Wu, J. Hu, and J. Liu, "Decentralized IoT Resource Monitoring and Scheduling Framework Based on Blockchain," IEEE Internet of Things Journal, vol. 10, no. 24, pp. 21135–21142, 2023.

[9] Q. Wang, S. Chen, and M. Wu, "Incentive-Aware Blockchain-Assisted Intelligent Edge Caching and Computation Offloading for IoT," Engineering, vol. 31, no. 12, pp. 127–138, 2023.

[10] M. Chowdhury, "Merit: An On-Demand IoT Service Delivery and Resource Scheduling Scheme for Federated Learning and Blockchain Empowered 6G Edge Networks with Reduced Time and Energy Cost," Int. J. of Ad Hoc and Ubiquitous Computing, vol. 44, no. 2, pp. 79–103, 2023.

[11] L. Zhao, J. Wang, J. Liu, and N. Kato, "Optimal Edge Resource Allocation in IoT-Based Smart Cities," *IEEE Network*, vol. 33, no. 2, pp. 30–36, Mar./Apr. 2019.

[12] N. Kherraf, H. A. Alameddine, S. Sharafeddine, C. M. Assi, and A. Ghrayeb, "Optimized Provisioning of Edge Computing Resources With Heterogeneous Workload in IoT Networks," *IEEE Transactions on Network and Service Management*, vol. 16, no. 2, pp. 459–472, 2019.

[13] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine Learning for Resource Management in Cellular and IoT Networks: Potentials, Current Solutions, and Open Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1251–1276, 2020.

[14] M. Alam, N. Ahmed, R. Matam, M. Mukherjee, and F. A. Barbhuiya, "SDN-Based Reconfigurable Edge Network Architecture for Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 10, no. 18, pp. 16494–16505, Sep. 2023.

[15] J. Okwuibe, J. Haavisto, I. Kovacevic, E. Harjula, I. Ahmad, J. Islam, and M. Ylianttila, "SDN-Enabled Resource Orchestration for Industrial IoT in Collaborative Edge-Cloud Networks," *IEEE Access*, vol. 9, pp. 115839–115851, Aug. 2021.