Non-Fungible Token Enabled Resource Trading Marketplace for 6G Network Slicing

Nisita Weerasinghe*, Pawani Porambage†, An Braeken‡, Madhusanka Liyanage§, Mika Ylianttila¶
*¶Centre for Wireless Communications, University of Oulu, Finland, †VTT Technical Research Centre, Finland
‡ Vrije Universiteit Brussel, Belgium, §School of Computer Science, University College Dublin, Ireland
*¶[firstname.lastname]@oulu.fi, †pawani.porambage@vtt.fi, ‡an.braeken@vub.be, §madhusanka@ucd.ie

***Abstract*—The shift from fifth generation (5G) to sixth generation (6G) networks is anticipated to significantly advance network slicing. This progress is driven by the growing demand for next-generation applications and services. However, these advancements must be managed within the constraints of limited resources. This evolution opens up opportunities for resource sharing through emerging marketplaces, yet it introduces various business and technical complexities that need to be addressed. Additionally, finding cost-effective solutions is also essential for the future of networks. In this paper, we propose a blockchain-based architecture that utilizes non-fungible tokens (NFTs) for the trading of network resources within the 6G network slicing. To the best of our knowledge, this is the first study to represent network resources as NFTs within the context of network slicing. The architecture employs NFTs to authenticate and manage various network resources, providing a decentralized platform for their secure creation, management, and exchange. Using resource NFTs, our system ensures more granular and flexible control over network resources than existing state-of-the-art systems, where NFTs are tied to network slices. We implemented a prototype of this system to validate its viability. Our performance evaluation confirms that the proposed approach is efficient and cost-effective compared to baseline models in managing network resources within network slicing. These findings highlight the potential of our system to transform network management practices and effectively meet the demands of future networks.**

***Index Terms*—5G, 6G, Network Slicing, Blockchain, NFTs**

I. INTRODUCTION

Network slicing is a concept first introduced in 5G networks. It involves dividing a single physical network into multiple independent logical networks, each tailored to meet specific service requirements [1]. This is achieved by managing and orchestrating a range of underlying resources such as bandwidth, storage, computing power. As we advance towards 6G technology, network slicing is expected to take on an even greater significance. It will likely support a wider range of applications, help reduce capital expenditures and operating expenses (CAPEX/OPEX) [2], and open up new revenue streams [3]. As a result, Communication Service Providers (CSPs), Network Slice Providers (NSPs), or Mobile Network Operators (MNOs) find it increasingly necessary to collaborate with a multitude of Infrastructure Network Providers (InPs) or other MNOs. Such multi-party collaboration is vital for accessing diverse resources, opening opportunities for both established and emerging players in the telecommunication industry to lease or share resources, thereby promoting an open ecosystem [4].

However, such an ecosystem is prone to challenges. **1) Trustworthiness issues:** Deploying end-to-end (E2E) slices, which is a made up of numerous resources and services, typically requires to undergo number of administrative negotiations among parties who may lack mutual trust. This often leads to the need for costly manual interventions, such as the use of neutral legal entities or intermediaries to facilitate fair dealings [3], [5]. **2) Complex orchestration:** Managing and coordinating multiple stakeholder interactions, transactions, and their billing processes are complicated [4], [6]. **3) Lack of accountability and transparency:** As competitiveness escalates in the open ecosystem, the risk of Service Level Agreement (SLA) breaches rises, often going unnoticed. Also, there are limited mechanisms to hold sellers accountable for their actions and enforce compliance effectively. Further, tenants often lack clarity on whether they are receiving the services as specified in their SLAs. This lack of accountability and transparency reduces the trust and confidence of tenants in the services they purchase. Hence, maintaining an enhanced Quality of Service (QoS) for end-users, a primary aim of 6G, becomes more challenging [2], [4]. **4) Traceability problems:** Network resource buyers may falsely claim ownership and resell purchased resources. This is due to the lack of a reliable mechanism to verify their origin and transaction history. Without a secure provenance record, the risk of fraudulent claims rises [7], [8].

This urges for a next-generation network resource management system that addresses all these challenges efficiently [3], [4], [7]. Blockchain technology comes in handy in maintaining trustworthy interactions, automating negotiations and providing immutable record-keeping. Whilst, integration of non-fungible token (NFT)-based tokenization techniques offer a promising approach to tackle challenges such as ownership tracking, provenance tracing, and auditability [7], [9]. A preliminary contribution in this area are the works by Bandara et al. [10], [11] which employs NFT tokenization for network slices (NSs). This method enhances the auditability and transparency of NSs by representing them as NFT tokens. Despite its advantages, this approach exhibits limitations in terms of flexibility and granularity. It primarily focuses on the NS level and does not extend to the lower resource level, leaving complexities in resource management unaddressed. In our proposal, aforementioned challenges are expected to be rectified and the key contributions of our work are as follows:

- We propose a novel architecture for a resource trading marketplace to simplify network resource management processes in 6G network slicing.
- We implement a prototype of the proposed system to evaluate its performance and confirm its viability in a real-world scenario.
- We conduct multiple comparative analyses of our proposed model against baseline models highlighting its advantages and discussing its potential to outperform.

The remainder of the article is outlined as follows. Section II reviews related works. Section III presents the proposed NFT-based marketplace architecture. Section IV provides a prototypical implementation and evaluates the performance of the proposal compared to baseline solutions. Finally, Section V includes the conclusion of the paper.

II. RELATED WORKS

The marketplace concept is evolving to meet the diverse needs of modern network resource management. A study by Yrjölä et al. [3], which involved the analysis of business model scenarios by sixty experts from major infrastructure manufacturers, operators, regulators, and academia worldwide, highlights the critical role of a transaction platform—a marketplace for all virtualized 6G network resources. Currently, the 5G Infrastructure Public Private Partnership (5G-PPP) has outlined a marketplace concept for network applications in one of its white papers [12]. The EVOLVED-5G Marketplace [13] provides support for network application creators through tools designed for building, certifying, and releasing network applications. However, these studies focus on common network application analysis and rely on centralized architectures, which introduce limitations like single points of failure, reduced transparency, and greater security vulnerabilities, overlooking the need for a trustworthy environment for all stakeholders.

Hence, researchers have turned to blockchain technology as a promising solution. Javed et al. [5] discuss the potential of integrating blockchain in 6G networks. Yrjölä et al. [6] propose decentralized business models for 6G networks with the use of blockchain, for trading virtualized network resources. In the paper by Nardini et al. [14], a blockchain-based decentralized electronic marketplace for computing resources is proposed. Similarly, Papadakis-Vlachopapadopoulos et al. [15] explore the orchestration of resources in edge clouds through a blockchain-based service marketplace. These marketplaces use smart contracts to automate cross-service communication and resource allocation between sellers and buyers.

To further advance the state-of-the-art in blockchain-based marketplace solutions, Zeydan et al. [7] advocate the incorporation of NFTs. Recently, researchers have shown a growing interest in integrating NFTs into network management. For instance, Shao et al. [9] highlight the use of NFTs in 6G wireless networks. Similarly, Han et al. [16] propose an NFT-based distributed auction mechanism for trading multiple computing resources within a network. Moreover, Bandara et al. [10] explore the application of NFTs to the management and brokerage of NSs in 5G/6G environments. Building on this, Bandara et al. [11] improve their system by integrating GPT-3.5 to make intelligent decisions in 5G/6G network slicing environments. However, these studies have not sufficiently focused on the individual resources that make up these slices, which may allow violations at the resource level to go unnoticed. Since ownership details are not thoroughly tracked, pinpointing the accountable stakeholder for violations becomes challenging, potentially degrading overall NS performance. Further, creating dynamic configurations for resources can be challenging as they are tightly coupled to the slice. Therefore, there is a clear demand for a well-designed NFT-based resource marketplace for 6G network slicing that effectively addresses all of these challenges.

III. PROPOSED ARCHITECTURE

This section introduces a novel architecture of an NFT-based resource marketplace and discusses its key participants, aligned with 3GPP specifications [1]. It then outlines the functionalities of the fundamental components of the system.

The proposed architecture for the NFT-based resource marketplace in 6G network slicing is illustrated in Figure 1. The diagram identifies four main entities: resource providers (orange) and resource consumers (yellow), who are the primary stakeholders interacting with the proposed system. External entities (dark green) are connected for resource verification and SLA monitoring. The core blockchain-based components (grey) of the marketplace are responsible for registration, brokering, trust management and billing.

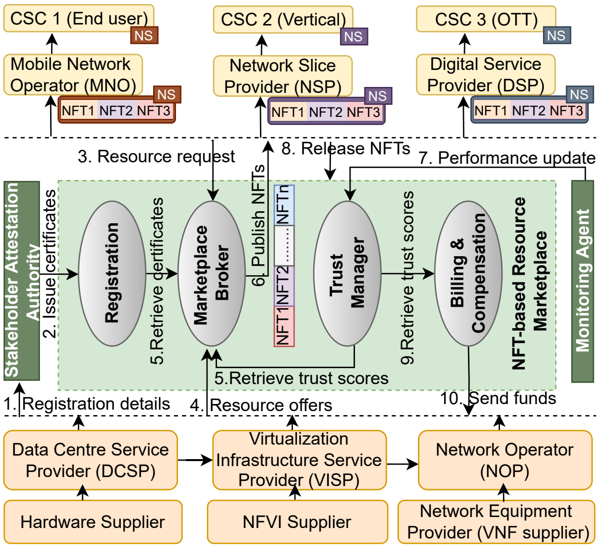

Fig. 1. Proposed Architecture of the NFT-based Resource Marketplace

Resource providers include entities such as Network Functions Virtualization Infrastructure (NFVI) providers, Virtual Network Function (VNF) providers, Network Operators (NOPs), Virtualization Infrastructure Service Provider (VISP), InPs [1]. These providers offer essential virtual resources and network functions. Resource consumers, such as NSPs, MNOs or Digital Service Providers (DSPs), utilize these resources to create NSs for Network Slice Customers (NSC), including end-verticals and Over-The-Top (OTT) service providers [1]. For instance, 5G core service providers purchase VNFs to deploy critical 5G network functions like the Session Management Function (SMF), User Plane Function (UPF), etc.

NSs are composed of service chains of VNFs, each carrying out specific tasks to meet diverse traffic requirements. VNFs, such as routers and firewalls, are individual network services that run as software on virtual machine (VM) or container instances on generic hardware. Each NS is governed by its own SLAs. In the proposed system, individual network resources (or VMs) are represented as NFTs. Each NFT contains metadata detailing the specifications of the resource, performance metrics, and ownership information. When resource buyers submit requests, the system perform resource brokering to select the optimal resource unit, tokenized as an NFT, from the marketplace. The resource buyer can then create customized NSs from the selected tokenized resources to fulfill their customer's specific needs.

A. Stakeholder Attestation Authority (SAA)

The SAA is a recognized certification entity that can function either as a third-party software on user devices or as an external auditor. Sellers must undergo this verification process upon on-boarding and whenever the seller's resource inventory changes. The key functions of the SAA include: 1) Resource verification: This process checks whether the hardware resources claimed by sellers are actually available, ensuring transparency and accuracy in listings. The SAA can employ software tools to remotely access and verify the specifications or conduct on-site inspections and remote audits. 2) Identity authentication: The SAA confirms the authenticity of seller identities, confirming they are who they claim to be. This authentication process, akin to the Know Your Customer (KYC) [17] procedure, is essential for mitigating identity theft and fraud within the marketplace. Upon successful verification, a certificate is issued to the seller as proof of authenticity.

B. Registration

The Registration component receives verified seller information from the SAA, and requires resource providers to submit details outlined in Table I. This includes details such as Computing Hardware (CH), Memory Hardware (MH), Storage Hardware (SH), and Networking Hardware (NH). Also, note that we use Geekbench Scores (GSs) [18] to provide a universal benchmark of CPU performance. Sellers must also specify the geographical and network locations of their resources, along with associated Overcommit Ratios (ORs) and Safety Margins (SMs) for each component. The OR expresses the proportion of resources allowed to be over-committed compared to the total available resources. SM represents an additional percentage added to account for unforeseen resource requirements. Sellers submit this information to the SAA (see subsection III-A), which performs verification and issues certificates based on the provided data. Note that the resource types listed in Table I are for illustrative purposes only. In real applications, these can be expanded to include more advanced resource types as required.

TABLE I
RESOURCE SELLER REGISTRATION PARAMETERS [16]

Name	Type	Unit	Value
Computing Hardware	CPU	GS [18]	uint
Memory Hardware	RAM	MB	uint
Storage Hardware	Disk	MB	uint
Networking Hardware	Bandwidth	Mbps	uint
Location	Geographical location	GPS	string
	Network location	IP address	string

The registration component calculates the Idle Resources (I), which are the remaining resources that are available for allocation. This calculation is performed for each Hardware Type (HT) of resource sellers based on the Available Hardware (A), as detailed in Equation 1.

$$I_{\text{HT}} = A_{\text{HT}} \times OR_{\text{HT}} \times (1 + SM_{\text{HT}}) \tag{1}$$

C. Marketplace Broker

The role of the marketplace broker commences when a buyer submits a resource request, specifying their needs alongside weighted priorities for price and trust score. Sellers, in response, provide offers tailored to these requests. Before submitting any tailored offers, sellers must pass through a mandatory verification process conducted by the marketplace broker. This initial step is to confirm that sellers have adequate resources to fulfill the requested services. The broker evaluates specific resource parameters against the seller's available capacities (I_{HT}) to ensure that offerings are viable and can proceed to the next stage without over-committing resources beyond set limits. Upon verification, the marketplace broker uses a scoring mechanism (Equation 2) to evaluate seller offers based on buyer priorities, including trust scores and pricing competitiveness, to identify the offer that best meets buyer preferences. The broker then selects the seller with the highest score, and facilitates the establishment of an agreement between the selected seller and the buyer.

$$\begin{aligned} SS_{\text{s}} = (1 - &\left[\frac{O_{\text{val}_s} - O_{\text{min}}}{O_{\text{max}} - O_{\text{min}}}\right]) \times W_{\text{P}} \\ &+ \left[\frac{TS_{\text{val}_s} - TS_{\text{min}}}{TS_{\text{max}} - TS_{\text{min}}}\right] \times W_{\text{TS}} \end{aligned} \tag{2}$$

Here, SS_{s} denotes the Selection Score of seller s, ranging from 0 to 1. O_{val_s} represents the offer value submitted by the seller, O_{min} and O_{max} represents the minimum and maximum offer values submitted by any seller, respectively. Similarly, TS_{val_s} refers to the trust score of seller s, with TS_{min} and TS_{max} indicating the minimum and maximum trust scores out of the trust scores of sellers who submitted offers. The weights W_{P} and W_{TS} reflect the buyer's prioritization of price and trust score, respectively, and the summation of weights is 1.

D. Monitoring Agent

The monitoring agent, continuously observes the sellers' activities, focusing particularly on their resource commitments and compliance with service metrics as stipulated in the SLAs. Monitoring is an ongoing process, and any deviations from the agreed performance levels are internally recorded as they occur. These records accumulate over time. At predetermined, regular intervals, the monitoring agent reviews the accumulated records, and if deviations are found, they are sent in batches to the trust manager. If no deviations are recorded, no transactions with the trust manager occur, reducing the frequency of transactions. However, at the conclusion of each contract, the monitoring agent submits an overall performance score of the service provided by the seller, to the trust manager. This score is then incorporated into the billing and compensation system to determine the overall compensation for the service.

E. Trust Manager

The trust manager, plays an important role in maintaining seller integrity and reliability within the platform, which will be invoked at four key stages.

1) Registration stage (see subsection III-B): Sellers receive an initial neutral trust score upon registration.

2) Verification stage (see subsection III-C): Before NFT creation, the trust manager evaluates the resource availability of the seller against requested amounts, taking into account permitted over-commitment levels. Insufficient resources are flagged, and the trust score of the seller is reduced accordingly.

3) Monitoring stage (see subsection III-D): During service delivery, committed resources are monitored for resource offerings, and service metrics are monitored through SLAs for service offerings. Any deviations from agreed standards result in a trust score deduction based on the severity of the violation.

4) Post-Contract Evaluation: At the end of the contract, sellers meeting or exceeding expectations receive a trust score increase, with a capped maximum limit.

F. Billing and Compensation

When a buyer purchases an NFT from a seller, the payment is held in escrow within a smart contract. Ownership of the NFT is transferred to the buyer for a specified period, during which the buyer uses the associated resources. At the end of this period, the NFT returns to the seller, and funds are released based on the seller's performance. If the seller meets the contract terms, the full payment is transferred to them. If not, compensation is provided to the buyer, and the remaining funds go to the seller based on the level of service delivered.

G. Network Resources Elasticity

Future 6G networks will prioritize dynamic user requirements, necessitating network resources elasticity [4]. When automatic scaling requests are detected, the monitoring agent will track resource usage, and the system will automatically allocate additional tokens from the marketplace to meet resource demands for the contract period. These new tokens will merge with existing ones to form an ensemble token, aggregating resources to handle increased workloads without manual intervention. For service migration, when virtualized elements are moved across different geographical locations, the system will release the token associated with the current location, and automatically create an equivalent token for the new location. The released token will be sold, and a new token will be purchased from a local vendor.

IV. PERFORMANCE STUDY

A. Simulation Analysis

We conducted an experiment using MATLAB to validate the effectiveness of the proposed trust-based system in comparison to state-of-the-art models [10], [11] for selecting honest sellers. The primary objective of this experiment was to evaluate the success rate of selecting an honest seller for a given buyer. The experiment involved a pool of hundred sellers, comprising both honest and dishonest entities. Trust scores and service costs were randomly assigned to each seller. To assess the systems, the percentage of dishonest sellers in the pool was varied in fifty steps, ranging from 0% to 50%, with increments of 1%. For each configuration, the average success rate was determined after simulating five-hundred buying instances.

In the state-of-the-art models, no specific emphasis was placed on the method of seller selection. Consequently, each seller had an equal probability of being chosen to supply resources for NS creation, regardless of their honesty. In contrast, the proposed trust-based system selects the best seller by considering both trust scores and service costs. Buyers assign weights to these attributes, which are used to rank sellers with valid offers. The seller with the highest rank is selected, giving an advantage to those with higher trust scores and lower service costs. As shown in Figure 2, the simulation results indicate that this approach significantly outperforms state-of-the-art models, especially as the proportion of dishonest sellers increases.

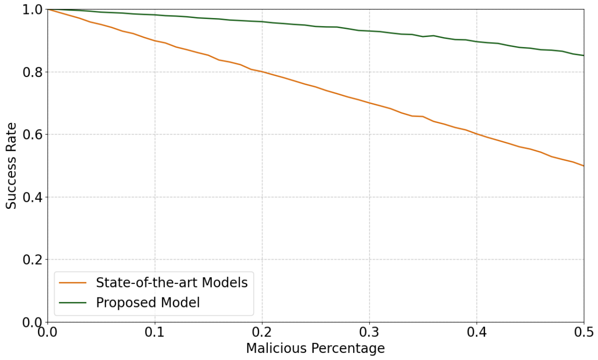

Fig. 2. Comparison of Seller Selection Strategies: State-of-the-art vs. Proposal

B. Experimental Setup

We have developed a proof of concept (PoC) implementation of our proposed approach on the Ethereum blockchain to illustrate its feasibility. We chose a public blockchain to handle growing user demand in future networks, offering accessibility for both large and small players. This PoC demonstrates our system model and is depicted in Figure 3. Within our implementation, smart contracts play a major role in automating blockchain-related tasks within the marketplace. These smart contracts are coded using Solidity, a programming language specifically tailored for Ethereum smart contracts. To execute our marketplace, we rely on a local Ethereum node provided by Hardhat. Additionally, we utilize the Openzeppelin library to implement the ERC721 token standard, which governs the ownership and secure transfer of NFTs on the Ethereum blockchain. Furthermore, we employ the Ownable and AccessControl Solidity libraries to effectively manage the roles and permissions of actors within the marketplace. In our PoC implementation, we have integrated InterPlanetary File System (IPFS) using Pinata, a service that simplifies hosting files on the IPFS network. With Pinata, we upload folders containing images and JSON files for our NFTs, each assigned a unique Content Identifier (CID). This CID allows easy retrieval of content from any IPFS node. Pinata also automatically updates the CID when content changes, ensuring users always access the most recent version.

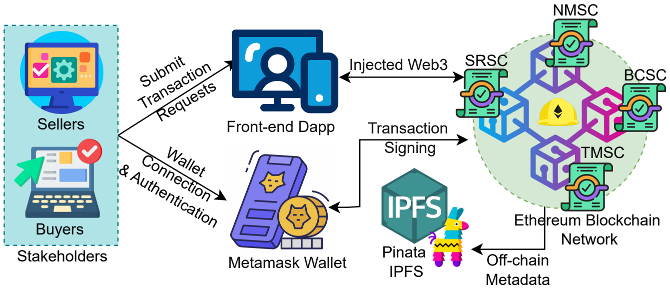

Fig. 3. Prototype setup of the NFT-based resource marketplace

The developed marketplace comprises four main smart contracts, each playing a pivotal role in executing the key functionalities outlined in the Section III. **1) Seller Registration Smart Contract (SRSC)** facilitates the onboarding and managing resource providers. Further, it provides insights into their capacity and availability. **2) NFT Minting Contract (NMSC)** initiates a verification procedure for NFT creation requests. Upon successful verification, it permits the creation of NFTs and publishes them in the marketplace. The associated data of these NFTs will be hosted on IPFS. **3) Billing and Compensation Smart Contract (BCSC)** handles the payment process for buying and releasing NFTs within the system. It facilitates the purchase of NFTs from sellers, guaranteeing that the correct payment amount is sent and setting an expiry time for NFT usage. Additionally, it handles releasing of NFTs back to their original owners after the contract period has ended, transferring the appropriate payment amount to them based on their trust score. **4) Trust Manager Smart Contract (TMSC)** conducts trust related operations to maintain trustworthiness and fairness between primary stakholders. It orchestrates the adjustment of trust scores of the sellers on monitoring reports provided by the monitoring agents. It guarantees that sellers adhere to the terms specified in their SLAs. In cases where sellers fail to meet these expectations, this contract reduces the possibility of selecting such sellers, by reducing their trust score.

C. Experimental Results

In this subsection, we evaluate the performance of a PoC implementation of the proposed architecture, focusing on cost metrics. We present a comprehensive analysis of the experimental results obtained, offering a comparison with closely related state-of-the-art systems [8], [10]. To make a fair assessment, we implemented and tested the most closely related work [10] on the Ethereum blockchain under identical conditions as our proposed system. Additionally, the cost analysis provided by the system discussed in [8] was carried out on a local Ethereum node, allowing for a direct comparison with our setup.

1) Gas Consumption: Transactions on the Ethereum blockchain require payment of gas fees to implement smart contracts. Gas measures the computational effort needed to execute computational operations on Ethereum. These fees, known as gas fees, are directly proportional to the consumed gas units. In our comparison of related state-of-the-art systems, we compare cost analyses conducted for an NFT data marketplace [8] and an NFT NS marketplace [10]. To ensure a fair comparison, we identified and aligned the key smart contracts and functionalities commonly found in NFT-based marketplace systems. Results are presented in Table II.

Our system demonstrates slightly reduced gas consumption for most functionalities when compared to the reference models, with the exception of asset management and token minting. The increased gas consumption in asset management is attributable to the additional features, such as the billing and seller rating mechanisms, managed by the BCSC and TMSC. For token minting, the higher gas costs in our system result from the comprehensive verification process conducted prior to minting any tokens. Additionally, while the model in [10] exhibits high gas consumption for token minting due to the expense of tokenizing an entire slice with multiple resources, both [8] and our system focus on tokenizing individual assets. Despite these differences, the overall costs for deploying smart contracts and executing key operations within the NFT marketplace are comparable between our system and the reference models.

TABLE II
COMPARISON OF GAS CONSUMPTION IN NFT-BASED MARKETPLACES

Smart Contract Deployment	**[8]**	**[10]**	**Ours**
Asset Owner Registration	3.9×10^6	1.6×10^6	1.5×10^6
Asset Minting	3.2×10^6	3.1×10^6	1.1×10^6
Asset Management	1.6×10^6	2.5×10^6	6.5×10^6
Token Trade Stages	**[8]**	**[10]**	**Ours**
Token Minting	1.4×10^5	1.5×10^6	2.8×10^5
Token Transfer	1.2×10^5	1.2×10^5	0.8×10^5
Token Release	1.6×10^5	1.8×10^5	0.4×10^5

2) Batch minting: In practical scenarios where there are frequent requests for the creation of multiple tokens, the cost of token minting can be significantly reduced by minting them in batches within a single transaction. In our study, we compared the proposed system with the baseline model [10], focusing on the creation of NS instances with varying numbers of resources per slice. The baseline approach involves four primary resources—RAN, core, transport, and cloud—per slice. Based on this configuration, we started our comparison with four resources per slice and then extended the analysis to slices containing six and eight resources.

In the proposed method, a single transaction was used to mint all resource tokens contained within a slice, and we compared the resulting costs with those of the baseline model. As illustrated in Fig. 4, our proposed method consistently outperforms the baseline model across all tested configurations, demonstrating lower gas costs. This suggests that the proposed solution offers potential financial advantages, making it a more cost-effective approach for network management, particularly in environments where cost efficiency is critical.

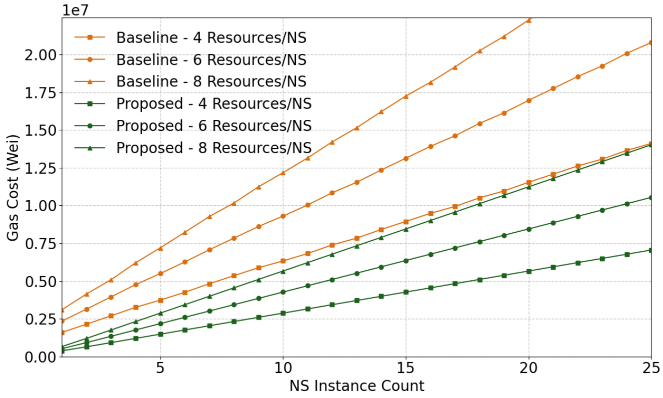

Fig. 4. Comparative analysis of gas consumption across NS instances

V. CONCLUSION

In this paper, we proposed a novel resource trading marketplace for 6G network slicing. Our model addresses key challenges in the current landscape. Using blockchain, it automates costly manual processes by removing intermediaries. This streamlines interactions among multiple stakeholders and guarantees fair resource orchestration and trustworthy negotiations. By integrating NFTs, our solution improves the traceability of resource ownership and enables resource-level auditability. It enhances seller accountability and allows for precise management of network resources. This reduces the risk of resource overcommitment and increases the trustworthiness and reliability of network operations. Our approach also increases the granularity and flexibility of network slicing compared to state-of-the-art models. It detects and reduces the impact of under-performing sellers, improving overall system performance. Our user-centric approach to the selection of sellers aligns with the main goals of 6G. It offers a better experience for end-users compared to baseline models. The PoC implementation, supported by both numerical and experimental analyses, demonstrates the effectiveness and viability of deploying these features within a single platform. The results confirm that our solution is more cost-effective than other baseline models, particularly in contract deployment, system functionality, and NS instance deployments. In general, our platform offers a novel, efficient, and cost-effective resource trading marketplace to the 6G networks, addressing current challenges. This also improves trust and confidence in all stakeholders involved. In the future, we plan to further enhance this architecture by incorporating auctioning systems to improve the overall efficiency of resource allocation.

ACKNOWLEDGEMENT

This research was supported by the Research Council of Finland (former Academy of Finland) 6G Flagship Programme (Grant Number: 346208), European Union in the CONFIDENTIAL-6G project (Grant ID. 101096435), Science Foundation Ireland under CONNECT phase 2 (Grant Number: 13/RC/2077_P2) project, and Cost action CA22104 Beingwise, and Vlaams Beleidsplan Cybersecurity 2024-2028.

REFERENCES

[1] 3GPP, TS 28.530, "5G; Management and Orchestration; Concepts, Use Cases and Requirements," 2021.

[2] S. Ebrahimi, F. Bouali, and O. C. Haas, "Resource management from single-domain 5g to end-to-end 6g network slicing: A survey," *IEEE Communications Surveys & Tutorials*, 2024.

[3] S. Yrjölä, "How could blockchain transform 6g towards open ecosystemic business models?" in *2020 IEEE international conference on communications workshops (ICC workshops)*. IEEE, 2020, pp. 1–6.

[4] F. Javed, K. Antevski, J. Mangues-Bafalluy, L. Giupponi, and C. J. Bernardos, "Distributed ledger technologies for network slicing: A survey," *IEEE Access*, vol. 10, pp. 19 412–19 442, 2022.

[5] F. Javed and J. Mangues-Bafalluy, "Blockchain and 6g networks: A use case for cost-efficient inter-provider smart contracts," in *2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2022, pp. 602–608.

[6] S. Yrjölä *et al.*, "Decentralized 6g business models," *Proceedings of the 6G Wirel. Summit, Levi, Finland*, pp. 5–7, 2019.

[7] E. Zeydan, L. Blanco, S. Barrachina-Muñoz, F. Rezazadeh, L. Vettori, and J. Mangues, "A marketplace solution for distributed network management and orchestration of slices," in *2023 19th International Conference on Network and Service Management*. IEEE, 2023.

[8] S. Ranjbar Alvar, M. Akbari, D. Yue, and Y. Zhang, "NFT-Based Data Marketplace with Digital Watermarking," in *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 2023, pp. 4756–4767.

[9] X. Shao, P. Cao, S. Wang, W. Wang, B. Zhou, and C. Sun, "Non-fungible token enabled spectrum sharing for 6g wireless networks," in *2023 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2023, pp. 1075–1080.

[10] E. Bandara, S. Shetty, R. Mukkamala, A. Rahman, P. Foytik, X. Liang, and N. W. Keong, "Kaputa - blockchain, non-fungible token and model card integrated 5g/6g network slice broker and marketplace," in *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, 2022, pp. 559–564.

[11] E. Bandara, P. Foytik, S. Shetty, R. Mukkamala, A. Rahman, X. Liang, N. W. Keong, and K. De Zoysa, "SliceGPT–OpenAI GPT-3.5 LLM, Blockchain and Non-Fungible Token Enabled Intelligent 5G/6G Network Slice Broker and Marketplace," in *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)*. IEEE, 2024.

[12] 5G-PPP Software Network Working Group, "Network applications: Opening up 5G and beyond networks version 2," *IEEE Access*, 2023.

[13] "Evolved-5G Marketplace," https://marketplace.evolved-5g.eu/, 2023, accessed: 2024-08-13.

[14] M. Nardini, S. Helmer, N. El Ioini, and C. Pahl, "A blockchain-based decentralized electronic marketplace for computing resources," *SN Computer Science*, vol. 1, no. 5, p. 251, 2020.

[15] K. Papadakis-Vlachopapadopoulos, I. Dimolitsas, D. Dechouniotis, E. E. Tsiropoulou, I. Roussaki, and S. Papavassiliou, "On blockchain-based cross-service communication and resource orchestration on edge clouds," in *Informatics*, vol. 8, no. 1. MDPI, 2021, p. 13.

[16] L. Han, R. Xie, Y. Ren, F. R. Yu, and T. Huang, "An nft-based distributed auction mechanism for multi-resource trading in computing power network," in *2022 IEEE 8th International Conference on Computer and Communications (ICCC)*. IEEE, 2022, pp. 528–532.

[17] N. K. Ostern and J. Riedel, "Know-your-customer (kyc) requirements for initial coin offerings," *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 551–567, 2021.

[18] S. Mustafa and K. Nanath, "Towards a model for performance evaluation of cloud machines," in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. IEEE, 2019, pp. 420–425.