Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 6, pp. 1891–1899
DOI : 10.47974/JIOS-2018

A blockchain-based auction framework for sustainable waste management : Utilizing non-fungible tokens (NFT) and zero knowledge proofs (ZKPs) for enhanced authentication

Ch Sree Kumar *
Akhilendra Pratap Singh †
Department of Computer Science and Engineering
National Institute of Technology Meghalaya
Laitumkhrah
Shillong 793003
Meghalaya
India

Abstract

The significant rise in Waste generation poses substantial difficulties for the management of it. A solution that ensures transparency, efficiency, and trust within the community is highly sought after as a means of addressing this issue. We proposed an advanced trading framework integrating Zero Knowledge Proofs (ZKPs), non-fungible tokens (NFTs), and blockchain technology with auction-based processing to enhance conventional waste disposal methods. In the proposed framework, with ZKPs, the organizations are verified in a decentralized system, where the authentication is carried out without disclosing sensitive information. Vendors can list the waste as NFTs on a secure marketplace, guaran teeing participation from accredited entities in the recycling process. Additionally, our framework implements an auction mechanism, enabling verified organizations to bid on waste materials. All transactions are stored on the blockchain, enhancing transparency, accountability, and trust among stakeholders. The performance of this framework is evaluated using Hyperledger Caliper, measuring critical parameters such as average latency, transactions per second (TPS), and memory consumption to ensure reliability and scalability.

Subject Classification: *68M14, 68Q87, 94A60.*

Keywords: *Sustainability, NFTs, Blockchain, ZKPs, Waste management, Auction mechanism, Decentralized system, Polygon, Metamask, Blockchain, Hyperledger caliper.*

* *ORCID-ID:* **0009-0008-5976-4298**
† *ORCID-ID:* **0000-0001-8840-4744**

* *E-mail:* **p21cs013@nitm.ac.in (Corresponding Author)**
† *E-mail:* **akhilendra.singh@nitm.ac.in**

1. Introduction

The quick rise in the waste generated from medical, residential, and commercial establishments poses a great challenge to effective waste management. Conventional waste disposal methods are ineffective as they compromise consumers' privacy, resulting in data breaches and unauthorized access. There is also a lack of transparency in waste management, which erodes trust. The centralized storage method also leads to scalability issues and fraud risks and thus demands more secure and transparent solutions. A groundbreaking solution is being provided by Blockchain technology to address the challenges by enhancing waste management efficiency, ensuring traceability, and providing better transparency throughout the entire process. Blockchain prevents unauthorized data modifications, ensuring data security in waste management. It also encourages greater public participation in recycling. Waste tracking becomes more precise by using Non Fungible Tokens (NFTs). The token-based incentives promote the token-based incentives. These digital assets help verify and authenticate waste disposal processes. Accountability is maintained between the waste producers and the recyclers. NFTs strongly reinforce the ethical, incentivized sustainable practices and sustainable waste management practices.

We have proposed a novel blockchain-based NFT framework-BNWaste designed to streamline recycling processes while enhancing security and transparency. The proposed framework connects verified organizations and stakeholders through an NFT- based system, ensuring only authorized participants can access and process waste materials. The framework incorporates an auction-based recyclable model, where recyclable waste is transparently listed and acquired by certified recyclers. These recyclers market the recycled products through our marketplace. Zero-knowledge proofs (ZKPs) are also employed to verify organizations while preserving their privacy. Thus enhancing security, reducing data exposure, and ensuring compliance with blockchain-based verification standards. Our framework - BNWaste, integrates ZKPs, Blockchain, and the Mina Protocol to establish a decentralized, secure, and scalable waste management system. Using our NFT marketplace, verified organizations can acquire waste from vendors or businesses, ensuring that recycling operations are conducted exclusively by certified entities. Key technological components of the framework include NFT storage for decentralized storage of digital assets, and seamless multi-wallet connectivity is provided by the Coinbase Wallet SDK & Web3Modal. Hyperledger Caliper measures

transaction throughput, average latency, and memory consumption to evaluate system performance, ensuring optimal efficiency and scalability. By integrating these advanced technologies, the BNWaste model mitigates the privacy risks and inefficiencies of traditional waste management and fosters a more sustainable and trustworthy waste disposal ecosystem.

The structure of paper is: 1: Introduction, 2: Review Literature 3: Proposed framework 4: Result discussion 5: Conclusion

2. Review Literature

This section reviews NFTs in various areas, including Blockchain technology and cryptographic-based verification, known as Zero Knowledge Proofs (ZKPs). Zero Knowledge Proof and blockchain technology have the potential to completely transform the waste management industry and the way the entire process is managed. Blockchain framework was proposed in [1] for effective waste management, integrating zero-knowledge proofs, NFTs, and Walrasian equilibrium to ensure transparency, trust, and efficiency. It employs cryptographic verification, equitable resource distribution, and immutable records, with performance assessed using Hyperledger Caliper. Author in [2] proposed a model where Zk-Auction is a decentralized blockchain-based auction system that prevents overbidding using zero-knowledge proofs to verify bidder funds without revealing identities. Blockchain, metaverse applications, security concerns, and sustainable technologies for an eco-friendly virtual future are discussed in [3, 4], and developed a framework that examines the potential of Blockchain in waste management in smart cities. In [5] examine the global waste management challenge, highlighting the importance of blockchain.

Supply chain management over the Blockchain has shown a promising benefit. In [6] propose an NFT-based blockchain-based marketplace to reuse and exchange electronic devices to address the growing e-waste crisis. Real-time tracking was discussed in [7] and monitoring in Industry 4.0 with sustainable SCM. Aslam et al. discuss a framework and its feasibility with the blockchain technology in [8]. Pakistan's oil industry's Supply chain analysis was carried out and the operational performance was discussed in greater detail. In [9, 10] thoroughly reviewed blockchain and supply chain management, and the work is classified by complexity. In [11], conducted a comprehensive literature review on blockchain platforms in global supply chain management. Token-based decentralized approach was proposed by [12] for upgrading cryptocurrencies less on

oracles, user registration, or KYC, ensuring fair pricing through decentralized auction simulations. Author in [13] discussed a unique auction mechanism using competition padding in energy trading to lower budget deficits. AB Crowd was developed by [14] which is based on crowdsourcing built on top of Ethereum, where an auction mechanism - Repeated- Single-Minded Bidder mechanism which is based on the trusted task allocation and truthful bidding incentives.

3. Proposed framework for NFT Blockchain in the waste management

We introduced a novel blockchain-based waste management framework to facilitate secure and transparent recycling exclusively among verified organizations as shown in Figure 1. Leveraging Zero-Knowledge Proofs (ZKPs), BNWaste ensures participant authenticity while enabling the auctioning of recyclable waste. Participation to authenticated waste management organizations through ZKPs, ensuring compliance and trust. The highest bidder acquires the waste, which is then processed through the marketplace, fostering a competitive and efficient recycling ecosystem

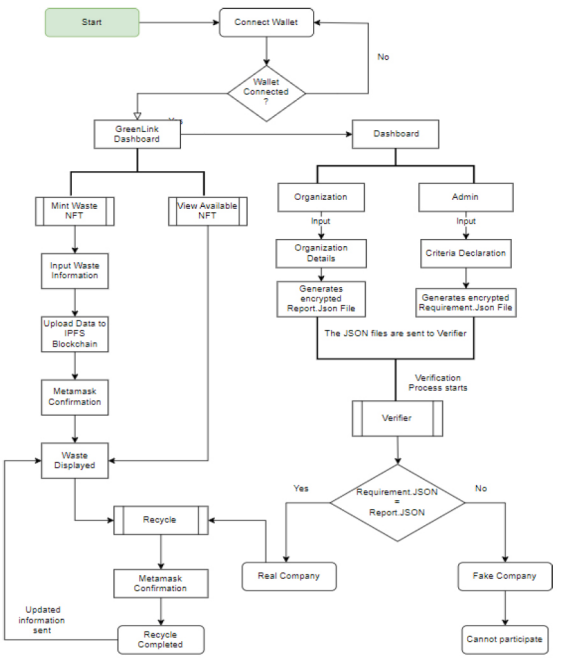

Figure 1

Flowchart of the proposed model

.

We chose a lightweight blockchain protocol – Mina which maintains a cryptographic snapshot of the ledger, optimizing scalability and efficiency. The auction-based system enables competitive pricing and secure transactions, enhancing market efficiency.

3.1 *Proposed framework's Algorithms*

Of the several algorithms used we show here Algorithm 1 presents the Zero Knowledge Proof. Algorithm 2 shows the Auction process.

Algorithm 1: Zero Knowledge Proof Verification (ZKPs)

Input: patient, secret, challenge
Output: true or false based on proof verification
Initialization
    Retrieve the unique secret associated from the database.
    Generate a random nonce $r \in Z$.
    Compute the commitment:
        $C = \text{Hash}(\text{secret}, r)$
    Send the commitment C to the verifier.
Verifier generates a random challenge $e \in Z$ and propagates it to the prover.
    Prover computes the response:
        $s = r + e \times \text{secret}$
    Send the response s to the verifier.
    Verifier reconstructs the expected commitment:
        $C' = \text{Hash}(\text{secret}, s - e \times \text{secret})$
    if $C' == C$ then
        Log: Verification successful. Identity confirmed.
        return true
    else
        Log: Verification failed. Potential tampering detected.
        return false
    end if
Audit - Log the verification result for future auditing and security checks.

Algorithm 2 AUCTION Process:

```
function AUCTION
    Notify the sellers, buyers to participate
    Buyer gives auction specification
    BidInLead = Pre – auctionprice
    if ETHADDR ==seller's addr AND TIME < DEADLINE then
        Add Bids as a valid transaction
    else
        Don't add transaction
    end if
    if BID_NEW ≤ (BidInLead – BIDDECREMENTAmt) then
        BidInLead = BID_NEW of respective seller
    else
        BidInLead = BidInLead
    end if
    if TIME > DEADLINE AND ETHADDR matches buyer's addr
    then
        Notify Auction closed to sellers and Inform the winning
        bid, Transfer the winning bid amount to the seller, Add
        Transaction
        else
            Do not perform Transaction
        end if
```

4. Result discussion

Hyperledger Caliper, a benchmarking tool, was used to evaluate the proposed model's real-world performance by measuring transaction speed, tokenization, CPU and memory usage, and scalability under an input load of approximately 5000 transactions shown in Table 1.

Table 1

summarizing key performance metrics of the four smart contracts under varying worker node configurations (1 to 5)

Smart Contract name	Send rate (TPS)	Avg Latency (s)	Throug-hput (TPS)	CPU% (max)	CPU% (avg)	Memory max in MB	Memory (avg) in MB	Traffic in MB	Traffic out in MB
create market item	1000	8.23	236.4	90.871	48.9863	786	734	12.42	27.88
	2000	8.22	237.2	89.161	48.3484	820	761	12.32	26.58
	3000	8.19	240.1	88.112	47.0254	888	765	12.62	28.52
	4000	8.18	241.9	87.162	45.0511	897	812	12.42	27.41
	5000	8.21	241.8	90.179	45.3457	983	861	12.42	27.78
create market sale	1000	9.84	226.4	22.666	2.1125	984	773	9.47	30.88
	2000	9.4	227.1	23.506	2.2154	987	799	9.33	29.88
	3000	9.31	229.4	24.501	2.5771	986	798	9.25	29.88
	4000	9.87	228.2	25.503	2.5985	982	837	9.45	30.88
	5000	9.8	230.6	26.909	2.6275	986	848	9.54	30.78
create token	1000	10.52	218.5	24.985	2.4914	20.815	11.21	11.62	32.18
	2000	10.56	216.4	25.351	2.5678	22.604	11.21	11.62	32.28
	3000	10.36	217.6	25.808	2.6155	22.514	11.01	11.42	31.28
	4000	10.52	218.8	26.798	2.7254	22.646	11.21	11.62	32.18
	5000	10.49	218.2	26.723	2.7871	22.771	11.31	11.72	32.08
fetch item listed	1000	9.98	215.2	20.174	1.9254	21.604	9.41	9.82	31.18
	2000	9.95	214.7	21.787	2.1658	22.209	9.31	9.72	31.08
	3000	9.54	216.4	23.509	2.2989	22.658	9.41	9.82	31.88
	4000	9.9	215.8	23.927	2.3175	22.638	9.31	9.78	30.97
	5000	9.98	215.5	25.38	2.5585	22.337	9.41	9.82	31.08

5. Conclusion

This research proposes a Blockchain-enabled Non-Fungible Token (NFT) and auction-based trading framework for sustainable waste management, utilizing Zero Knowledge Proofs (ZKPs) for validity. The framework facilitates waste minting, marketplace listing, ownership transfer, and item fetching with a user-friendly, reliable, transparent, and secure GUI. Performance analysis shows create Market Item has the highest throughput, averaging 241.9 s, and the throughput is lowest for the create Token function at 216.4 s for the fetch item contract. The average memory consumption of create Market Item and create Market Sale lies in

the range of 734-861 MB for the range of TPS from 1000-5000. The % Maximum CPU utilization of the four smart contracts lies in the range of 87 MB to 90 MB, 22.0 to 26.0 MB, 24.0 to 26.0 MB and 20.0 to 25.0 MB. Future work would compromise the interoperability of blockchain networks to facilitate cross-platform asset ownership and waste tracking.

References

[1] H. Garg, S. Jhunthra, R. Goel, S. Sharma, V. Gupta, R. Sharma, and P. Dass, "Understanding user polarisation regarding COVID-19 vaccines through social network analysis," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 8, pp. 2301–2336 (2024).

[2] R. S. Teppawar, R. N. Ingle, and R. A. Muneshwar, "Analysis of system of fractional partial differential equations using Laplace reduced differential transform with decomposition method," *Journal of Statistics and Management Systems*, vol. 27, no. 8, pp. 1577–1594 (2024).

[3] B. Shilpa, P. R. Kumar, and R. K. Jha, "LoRa DL: A deep learning model for enhancing the data transmission over LoRa using autoencoder," *The Journal of Supercomputing,* vol. 79, pp. 17079–17097 (2023).

[4] A. Arditi, P. Garimidi, D. Hirsch, and I. Milionis, "An initial framework for NFT auction mechanism design: Impossibility results and solutions," *Foundations of Blockchains*, COMS 6998-006, Columbia University, pp. 1–24 (2021).

[5] S. Sharma, A. K. Patel, and N. Menaria, "Integral transform of product of generalized k-Bessel function and generalized Hurwitz-Lerch Zeta function," *Journal of Interdisciplinary Mathematics*, vol. 27, no. 8, pp. 1757–1764 (2024).

[6] T. K. Mohammed, D. N. Vasundhara, S. H. Mehanoor, E. Sreedevi, P. R. Kumar, C. Manihass, and S. F. Baba, "A novel fusion approach for advancement in crime prediction and forecasting using hybridization of ARIMA and recurrent neural networks," *Journal of Information Systems Engineering and Management*, vol. 10, no. 38, pp. 404–420 (2025).

[7] B. Shilpa, P. R. Kumar, and R. K. Jha, "Spreading factor optimization for interference mitigation in dense indoor LoRa networks," in Proc. IEEE IAS Glob. Conf. Emerg. Technol. (GlobConET), pp. 1–5 (2023).

[8] J. Aslam, A. Saleem, N. T. Khan, and Y. B. Kim, "Factors influencing blockchain adoption in supply chain management practices: A study

based on the oil industry," *J. Innov. Knowl.,* vol. 6, no. 2, pp. 124–134 (2021).

[9] P. R. Kumar and B. Shilpa, "An IoT-based smart healthcare system with edge intelligence computing," in Reconnoitering the Landscape of Edge Intelligence in Healthcare, CRC Press, pp. 31–46 (2024).

[10] K. Duan, G. Pang, and Y. Lin, "Exploring the current status and future opportunities of blockchain technology adoption and application in supply chain management," *J. Digit. Econ*. (2024).

[11] P. Dudczyk, J. Dunston, and G. V. Crosby, "Blockchain technology for global supply chain management: A survey of applications, challenges, opportunities & implications," IEEE Access (2024).

[12] M. Rodinko, R. Oliynykov, and A. Nastenko, "Decentralized proof-of-burn auction for secure cryptocurrency upgrade," *Blockchain: Res. Appl.,* vol. 5, no. 1, pp. 100170 (2024).

[13] M. R. Z. E. Deen and G. M. Elmahdy, "Different types of odd harmonious labeling of super subdivision of various graphs," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 8, pp. 2373–2407 (2024).

[14] G. B. Mohammad, Shitharth, and P. R. Kumar, "Integrated machine learning model for URL phishing detection," *International Journal of Grid and Distributed Computing,* vol. 14, no. 1, pp. 513–529 (2021).

Received December, 2024