Akshitha Katkeri, 2025, 13:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Block Bazaar: NFT and Smart Contract Driven E-Commerce Platform

Akshitha Katkeri, Pallavi C V, Namitha R, Pratyusha C, Rekha Parashuram Pujari
Computer Science and Engineering BNM Institute of Technology Bengaluru, India

Abstract- BlockBazaar is this new decentralized marketplace thing that mixes NFT trading with regular e-commerce stuff. It runs on Ethereum smart contracts and has live auctions that work across different devices. You log in using MetaMask wallets, which keeps things pretty secure from the start. Access levels depend on your role in the system, you know how that goes.The security side uses hardened smart contract patterns to block common attacks like reentrancy issues or front- running scams. Every transaction gets recorded publicly through blockchain explorers, so there's full visibility into what's happening. The whole setup cuts out a lot of traditional cloud services while keeping user privacy tight. Testing shows these decentralized platforms can actually handle enterprise-grade security requirements without slowing things down. Response times stay quick even during peak usage, which matters for real-world shopping scenarios. Users get familiar interfaces that don't sacrifice blockchain's core benefits like permanent records and trustless transactions. The key takeaway here is that hybrid systems can bridge Web3 tech with conventional e-commerce needs effectively. Performance metrics match centralized competitors while maintaining cryptographic proof of ownership for digital assets.

Keywords - Non-Fungible Tokens(NFTs), Blockchain, Ethereum, Wallet , Smart ContractsBased Anonymization, Big Data Privacy.

I. INTRODUCTION

In the fast-changing world of digital business and blockchain technology, decentralized marketplaces are rising as a revolutionary new option to the old-style centralized e-commerce websites. Leveraging the natural advantages of blockchain technology, including immutability, transparency, and trustless transactions, these systems offer improved security, lower intermediary fees, and verifiable ownership tracking. However, the growing sophistication of blockchain-based attacks, including reentrancy attacks, front-running attacks, and smart contract bugs, poses significant threats to the security and integrity of decentralized marketplaces. As malicious players continue to create more advanced attack vectors aimed at smart contracts and blockchain infrastructure, it is ever more important to create strong and explainable decentralized systems that can effectively resist such adversarial inputs without compromising user trust and system performance.

In this work, we present a general description of decentralized NFT marketplace systems with focus on smart contract security, auction systems in real-time, and incorporation of blockchain transparency models for verifiable marketplace operation. We show and analyze our own implementation, BlockBazaar: a Security-Robust Decentralized NFT Marketplace based on multi-modal blockchain interactions, real-time auction systems with WebSocket support, and transparent decision-making

systems through detailed transaction logs and blockchain explorer integration. We accomplish this uniquely by implementing our system on several platforms such as web applications, mobile apps, and embedded systems, allowing for smart monitoring of market activities, sending instant notifications through real-time communication channels, and offering complete user experiences through React-based interfaces and React Native mobile apps. Our research shows how principles of blockchain transparency can be used to establish user trust in decentralized decision-making within an operational marketplace system by integrating both theoretical innovations in smart contract security and practical deployment methods in a wide range of computing environments. The survey further places our system in the context of the literature on blockchain security and decentralized commerce and identifies areas where the literature falls short and what future research should move toward in terms of developing secure and transparent systems for digital asset marketplaces.

II. RELATED WORK

NFT Marketplaces and Architectures

Decentralized NFT marketplaces became the focal point of blockchain-based digital trade. The NFT Marketplace project report [1] showcased how minting, listing, and royalty mechanisms could be incorporated into a decentralized platform. Building upon this, "The Future of E-Commerce: Integrating Blockchain, AI, and NFTs" [2] highlighted the potential of NFTs in supporting digital ownership and AI-driven personalization, delivering a secure and smart e-commerce space. Razi et al. [3] provided an extensive overview of NFT applications, including the issues of scalability, interoperability, and changing standards.

Smart Contracts and Auction Mechanisms

Smart contracts are the basis for trustless automation of digital markets. Decentralized auction work [4] demonstrated that sealed-bid and open auctions can be implemented securely with blockchain. A blockchain bidding model based on a tree-structured blockchain [5] enhanced scalability, whereas Singh et al. [6] designed a blockchain-enabled auction framework for location-aware services. Overall, these studies establish that fraud is mitigated, transparency is provided, and programmable business logic is enabled in e-commerce by smart contracts.

NFTs for Data Monetization and Access Control

NFTs are also being used in data security and monetization outside collectibles. Madine et al. [7] suggested a time- bound NFT framework, where encrypted data is retrieved for an expiry period, thereby monetizing sensitive information. This scheme illustrates uses in private data sets, subscription-based access, and premium content delivery. In the same way, incorporation of NFTs into e-commerce for supply chains [8] ensures product traceability, authenticity confirmation, and consumer confidence**.**

Security, Trust, and Legal Perspectives

The integrity of NFT platforms relies on robust security and regulation. Taherdoost [9] critically examined smart contracts and their vulnerabilities, including oracle failures, contract bugs, and privacy concerns, and proposed methodologies like formal verification and auditing. Bloomfield and O'Hara [10] examined transparency in markets and presented trade-offs between openness and competitive efficiency, which extend to NFT marketplaces that reveal provenance data. Legal viewpoints also underscore integrating smart contracts with conventional terms of service for the sake of enforceability in actual business.

Integration of AI and Blockchain in Marketplaces

By integrating blockchain and AI, trust and efficiency in online commerce are enhanced. Kumar and Dubey [11] proved how analytics driven by AI, coupled with blockchain transparency, can make fraud detection stronger and dynamic pricing more effective. Other research [12] focused on AI-driven supply chain optimization, illustrating how blockchain ensures data integrity while AI forecasts demand and enhances logistics. Such research supports that AI-blockchain fusion is a central force for the future of marketplaces powered by NFT.

Hybrid and User-Centric Deployments

Hybrid models integrating decentralization, explainability, and light deployment are becoming more popular. Chincheti et al. [13] presented a secure online auction system that traded-off blockchain trust with good design. Vogue Business [14] suggested "Web2.5" adoption tactics like custodial wallets and off-chain indexing to enhance user onboarding without compromising ownership transparency. These methods emphasize building systems that are secure and easy to use so that NFT e-commerce platforms can be adopted in the real world.

Table I. Comparison Based On Market Places

Feature / System	*Traditional E-Commerce*	*Blockchain- Only Marketplaces*	*Proposed Work (BlockBazaar)*
Primary Paradigm	Centralized servers with payment gateways	On-chain transactions, basic NFT minting	Hybrid (NFT + Smart Contracts + AI)
Transparen cy	Low (controlled by central authority)	Medium (on-chain but limited analytics)	Very High (immutable records + explainable AI insights)
Security	Vulnerable to fraud, data leaks	Resistant to tampering but prone to contract bugs	Strong (audited smart contracts + encrypted metadata)
Trust Mechanis m	Third-party intermediaries	Blockchain consensus only	Combined (Smart Contracts + AI-based fraud detection)
User Accessibili ty	Easy (email / password login)	Requires wallets, technical know-how	Web2.5 UX (custodial/non-custodial wallets, simplified onboarding)

III. PROPOSED METHODOLOGY

In this section, we discuss the underlying theory that supports the design and specify the prime mechanisms that will define our secure NFT and smart contract-driven e- commerce approach. We take advantage of blockchain combined with decentralized storage, wallet-based authentication, and automated smart contract execution in order to provide more secure transactions and useful transparency to users in an optimized way for scalability in various contexts.

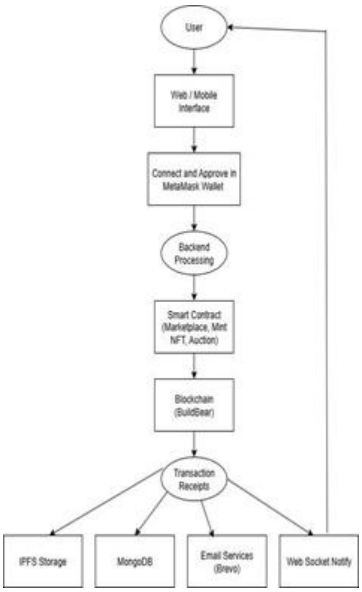

Fig.1. Flowchart

User Interaction and Wallet Approval

The system originated as a user interface via web or mobile. This is the start point where the customer can browse, transact, or interact with the marketplace. In order to execute any operation, the user is required to connect and approve the transaction with the MetaMask wallet for security purposes. Wallet-based authorization method needs to utilize decentralized credentials, yet validates that only the rightful owner, is allowed to transact for purchases, mint NFTs, or buy items via auction. The cryptographic signatures from MetaMask build trust and certify ownership in a completely decentralized way.

Backend Processing and Smart Contracts

Following approval from the wallet, your request has progressed to backend processing, where transaction validation and optimization are performed. Once validated, the system invokes smart contracts to control significant features of the smart marketplace. Those features include minting NFTs, transferring ownership, conducting auctions, and executing agreements for purchase. Since the contracts are self-executing and tamper-proof, the wallet can assist with special requirements instead of needing intermediaries, which allows for transparent, secure, and trustless transactions. This step reflects the crux of the system's philosophy.

Blockchain Deployment

The blockchain documents and verifies the executions of smart contracts, as shown by the BuildBear network. The blockchain offers immutability, consensus-based validation, and public transparency. Each interaction becomes a part of the distributed ledger, allowing for a permanent record of property ownership, payments, and auction results that cannot be changed or falsified. This contributes to accountability and trust in the e-commerce context.

Post-Transaction Processing

When the blockchain has validated a transaction, it creates receipts that will be passed on, and integrated into many services. One of those services is IPFS storage for decentralized assets and metadata. Another service is MongoDB to provide off-chain structured records. A third service is the Brevo email services for purchase confirmations and updates. A fourth, and final service is Web Socket services for providing the user live updates for their transaction. We believe that this multimodal approach is useful in that users will gain decentralized trust through the blockchain, but also the practicality of usability via accessible storage, communication, and live updates.

IV. IMPLEMENTATION

The suggested system is also modular in the sense of privacy and the application of decentralized blockchain with off-chain services all within a single e-commerce authorization mechanism. The novelty is a mechanism that combines wallet-based authentication, tamper-proof smart contracts that are automatically executed, and decentralized storage that is run in combination with scalable backend services and for real-time usability.

Multi-Modal Input Processing

The system allows for all blockchain, IPFS, MongoDB, and notification services to be independently sci-synchronized and participative channels, then commonized at the transaction level for format standards, data validation, and input conditions. This separation allows each service to remain, process type while capturing in common output. Integrations occur at the decision level rather than at data fusion, which would create inefficiency and noise. This layer approach for integrated architecture allows for maximum modularity and cross-verification, assuring consistency over decentralized and off-chain services.

Adversarial Robustness

To provide all these, the security of such attacks as fraudulent transactions, reentrancy issues, and adversarial manipulation in smart contracts ought to be reduced through training and testing contracts in real and adversarial situations. It is not done superficially through a quick set of filters but rigorous deployment in a testnet like BuildBear, where contracts are purposely engineered to accept edge cases and simulated exploits. This helps inform the internal discretization of the platform, providing

the ability to differentiate legitimate transactions from malevolent ones. The operation model can therefore establish stable transactional boundaries that are less likely to be breached from adversarial users or systemic vulnerabilities.

Explainability Of The Support Of Decision

One of the most prominent aspects of the BlockBazaar platform is its approach to explanatory transaction support as part of the marketplace ecosystem. Interpretability manifests in the modalities of output shares of each smart contract that are communicated in natural, and verifiable, patterns. Within the blockchain stream, the transaction receipt shows the exact function of the smart contract and block confirmation that generated the success of execution. Within the off-chain stream, Brevo email services and WebSocket notifications offer insightful clarity on the status of each stage of the transaction such as bidding closed, NFT minted, or payment received.

These clarifications are not just secondary enhancements, but rather part of the decision framework for the system, independent of the underlying smart contracts, which aid in both diagnostic awareness and ethical accountability in e-commerce applications that contain personal uses.

Localized Processing and Privacy Compliance

As opposed to conventional cloud-based commerce systems, this implementation focuses on decentralization and local ownership of assets. Wallet authentication, transaction signing, and asset control remain entirely in the hands of the user through MetaMask, ensuring no third-party custody. At the same time, blockchain execution, decision logic, and storage references are processed across decentralized and embedded infrastructures.

This architecture guarantees:

- Privacy of data, since no user funds or NFT assets are controlled by a central authority.
- Even in offline surroundings, users maintain operational independence, with confirmations visible once reconnected to the blockchain.
- Energy efficiency and scalability, as IPFS and MongoDB provide lightweight yet resilient data handling, suited to be used continuously in low-resource environments while maintaining decentralized sovereignty.

V. CONCLUSION

In this paper, we present a new decentralized e-commerce system, combining NFT minting, blockchain-ifified transactions with automated smart contracts to strengthen the security, transparency, and trustworthiness of online marketplaces. The use of smart contracts that have undergone testing in adversarial settings also provides greater resiliency to fraudulent behavior. Explanatory services such as transaction receipts, real-time updates, and email confirmations, together provide interpretability for commerce-related decisions. Unlike centralized e-commerce systems with third-party payment processors, this solution runs on a decentralized blockchain infrastructure, preserving user privacy and self-sovereignty. Additionally, the system simultaneously affords a balance of immutability and usability and features modular integration of storage and notifications to serve e- commerce demands in rapidly changing NFT-driven digital economies.

REFERENCES

1. NFT Marketplace, Project Report (PDF).
2. The Future of E-Commerce: Integrating Blockchain, AI, and NFTs for a Secure Digital Marketplace, Project Report (PDF).
3. Q. Razi, A. Devrani, H. Abhyankar, et al., "Non-Fungible Tokens (NFTs): Survey of Current Applications, Evolution and Future Directions," IEEE Open Journal of the Communications Society, vol. 4,pp.1201–1219,2023. https://www.researchgate.net/publication/376622455
4. I. A. Omar, H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Implementing Decentralized Auctions Using Blockchain Smart Contracts," Technological Forecasting and Social Change, vol. 168, 2021.

https://ieeexplore.ieee.org/document/10147205

5. A. Al-Madani, M. Alharbi, and K. Alotaibi, "Tree-Structure Based Improved Blockchain Framework for Secure Online Bidding," Journal of King Saud University – Computer and Information Sciences, 2024. https://ieeexplore.ieee.org/document/10363651
6. R. Singh, V. Sharma, and P. Kumar, "Blockchain-Based Auction Framework for Location-Aware Services," IEEE Access, vol. 11, 2023. https://ieeexplore.ieee.org/document/10068327
7. M. Madine, H. Al-Debagy, and Y. Jararweh, "Blockchain and NFTs for Time-Bound Access and Monetization of Private Data," IEEE Access, vol. 10, pp. 93592–93605, 2022. https://www.researchgate.net/publication/363257478
8. H. Treiblmaier and R. Beck, "The Impact of Blockchain on E- Commerce and Supply Chains," Technological Forecasting and Social Change, vol. 173, 2021. https://www.sciencedirect.com/science/article/abs/pii/S0040162521002 183
9. H.Taherdoost, "Smart Contracts in Blockchain Technology: A Critical Review," Information, vol. 14, no.2,pp.56–69,2023. https://www.researchgate.net/publication/368500729
10. R. Bloomfield and M. O'Hara, "Can Transparent Markets Survive?," Journal of Financial Economics, vol. 55, no. 3, pp. 425–459, 2000. https://www.sciencedirect.com/science/article/pii/S0304405X990005 62
11. S. Kumar and S. Dubey, "Integrating Blockchain and AI for Transparency, Security, and Efficiency in E-Commerce Supply Chains,"ResearchGate,2024. https://www.researchgate.net/publication/376622455
12. A. Gupta, V. Singh, and P. Mehta, "Supply Chain Optimization in E- Commerce: The Role of AI, Big Data, and Blockchain," Futures, vol. 140,2023. https://www.sciencedirect.com/science/article/abs/pii/S004016252100 2183
13. A. Chincheti, R. Dixit, V. Athavale, et al., "A Safe and Secure Online System for Bidding Using Blockchain Technology," Springer LNNS, 2024. https://www.researchgate.net/publication/384957839
14. Vogue Business, "The Fashion Exec's Guide to Web3: Building
Trust in NFT-Driven Commerce," Vogue Business Insights, 2022