BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2025
http://excel.fit.vutbr.cz

Online auctions using smart contracts

Anna Udvaros*

Abstract

In today's digital world, security, real-time response, and trust are key elements in online transactions, but traditional systems often rely on vulnerable third-party intermediaries. Smart contracts deployed on blockchain provide a decentralized and secure alternative by automatically verifying and enforcing contract terms without human intervention. The implemented online auction platform based on Solidity smart contracts demonstrates how decentralized technologies enable secure, transparent bidding and payment processing on the Ethereum network. The platform overcomes the disadvantages of traditional auction systems by strengthening transaction integrity, increasing reliability, and improving user experience in online marketplaces [1, 2, 3].

*xudvar02@fit.vut.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

In the rapidly changing digital landscape, online platforms handling financial transactions require seamless, reliable, and fraud-protected systems. Traditional centralized approaches introduce vulnerabilities including potential bias, human error, and privacy risks that undermine user trust and platform integrity [3].

This work addresses the need for transparent, tamper-resistant online auction systems that eliminate reliance on third-party intermediaries while maintaining transaction security and user trust. A successful solution must automate verification processes, provide real-time monitoring, and ensure equitable participation.

Current literature presents several theoretical models and partial implementations for blockchain-based auctions. Zhou et al. [4] proposed a basic auction framework using Ethereum but focused only on bidding mechanisms without addressing user authentication. Similarly, Kumar and Singh [5] demonstrated auction contract snippets but lacked comprehensive integration with cryptocurrency wallets. Existing commercial applications like OpenSea primarily target NFT auctions rather than general-purpose auction systems, while traditional platforms such as eBay continue relying on centralized verification processes susceptible to manipulation and delays.

The thesis proposes a complete, operational Ethereum-based auction platform that extends beyond theoretical models to provide a fully integrated system. Our implementation leverages Solidity smart contracts for automated bidding, payment processing, and auction verification while incorporating Ethereum wallet authentication for secure identity management [1, 2]. Unlike partial solutions in existing literature, this system demonstrates end-to-end functionality from auction creation through bid placement to final settlement, all managed through decentralized blockchain transactions.

My work demonstrates a practical application of blockchain technology that eliminates intermediaries while enhancing transaction transparency and security. The implementation showcases how smart contracts can be effectively deployed to create efficient digital marketplaces with immutable transaction records and automated enforcement [3].

2. Smart Contract Architecture

My auction platform utilizes a modular smart contract architecture deployed on the Ethereum blockchain. The contracts handle core auction functionality including bid processing, winner determination, and fund transfers without intermediaries. This section outlines the design principles and implementation details of the smart contract system.

2.1 Wallet Integration and User Authentication

The platform employs Ethereum wallets for secure user authentication and fund management. I implemented a cryptographic verification process that ensures users maintain full control of their assets throughout the auction process while providing secure identity verification. The system uses cryptographic signatures to verify wallet ownership - users sign a unique message containing a nonce (preventing replay attacks), and the platform verifies this signature against the claimed Ethereum address [2]. This approach creates a secure authentication environment without requiring users to surrender control of their funds to the platform. After registration, users must complete this wallet verification process before they can place bids or create auctions.

2.2 Transaction Flow and Security Measures

All actions within the auction platform—from initial listing to final payment—are recorded on the blockchain, creating an immutable audit trail [1]. The smart contract implements security measures against common auction vulnerabilities including shill bidding, bid sniping, and non-payment after winning.

2.3 Bidding Process and Fund Handling

Only users with verified Ethereum wallets are allowed to participate in bidding. Once an auction is active, users can place bids by sending the specified amount of Ether directly to the smart contract. The contract tracks the current highest bid for each user and ensures that only their highest valid bid is held in the contract balance.

When a bidder places a higher bid after already having participated, the smart contract automatically refunds the difference between the new bid and their previous bid. This mechanism ensures that the contract only holds each bidder's actual maximum contribution and minimizes unnecessary fund locking.

Upon auction conclusion, the winning bidder's amount is held by the contract until the seller manually ends the auction. Once the shipment is confirmed and the buyer acknowledges receipt, the contract automatically transfers the funds to the seller. All non-winning participants can securely withdraw their locked funds, with a gas fee applied during withdrawals to cover transaction costs. This secure, automated process ensures transparency, conditional settlement, and fairness for all participants.

3. Conclusions

My thesis demonstrates that smart contracts can effectively address the inefficiencies and vulnerabilities present in traditional online auction systems. By implementing a functional auction platform on Ethereum, I've shown how blockchain technology can be leveraged to create transparent, secure, and autonomous digital marketplaces [3]. Future work could explore scalability solutions, cross-chain compatibility, and enhanced privacy features while maintaining the core benefits of decentralization.

Acknowledgements

I would like to thank my supervisor Mgr. Kamil Malinka, Ph.D. for his guidance throughout this thesis project.

References

[1] Vitalik Buterin. A next-generation smart contract and decentralized application platform, 2014. Ethereum White Paper.

[2] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger, 2014. Ethereum Project Yellow Paper.

[3] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *IEEE International Congress on Big Data*, pages 557–564. IEEE, 2017.

[4] Yuyang Zhou, Mingyue Han, Linjie Liu, Jianfeng S. He, and Yanhua Wang. A secure auction system based on blockchain and smart contract. In *IEEE International Conference on Smart Internet of Things*, pages 206–211. IEEE, 2018.

[5] Ajay Kumar and Mandeep Singh. Secure bidding and payment system for online auctions using blockchain. *Journal of Information Security and Applications*, 52:102471, 2020.