



“A Survey Paper On EtherLuck: Decentralized Lottery System” A Literature review

Prashanth H S¹, Lalithya S², Lipika J³, Manasvi H Y⁴, Megha S⁵

Assistant Professor, Dept. of Computer Science and Engineering, K. S. Institute of Technology, Bengaluru¹

VI sem, Dept. of Computer Science and Engineering, K. S. Institute of Technology, Bengaluru²⁻⁵

Abstract: The Blockchain-Based Lottery System delivers reliability and empirical services while ensuring transparency and fairness. Moreover, system security uses a tamper-only distributed counter and Smart Contracts. In addition, the Lottery System allows active participants to fully execute advanced bypass verification and authentication protocols which ensure system integrity. The participation rules of the lottery and the award distribution mechanisms are programmed in the smart contracts that govern the Ethereum blockchain which is the bedrock of the system. As a lottery system, it favors speed of transactions over delays when using Ethereum funds to disburse prizes and tickets. This system is flexible because of dependence on Ethereum's robust ecosystem and scale easily, remaining the ideal fundamental for lottery frameworks that proliferate endlessly. It will focus on the user experience, the technology underpinning it, and the innovative horizon of the lottery systems based on blockchain technology to show how these systems can radically change the lottery ecosystem.

Keywords : Blockchain, lottery system, transparency, smart contracts, ethereum, distributed ledger, scalability, security, decentralized system, cryptocurrency.

I. INTRODUCTION

1.1 Background and Motivation

1.2 The lure of life-changing prizes has made lotteries a mass attraction for centuries. However, allegations of fairness and tampering have eroded trust in traditional lottery systems. Blockchain technology has transformed the lottery industry by providing an open, decentralized, and tamper-proof platform. Blockchain lotteries ensure the integrity of the lottery system, eliminating single points of control and ensuring randomness of winning numbers.

Blockchain technology offers a safe and reliable platform for lotteries where it is feasible to create reliable lottery systems. These systems offer fairness, transparency, immutability, and verifiability, allowing users to independently validate results and building trust. The use of blockchain technology in lottery operations has the ability to revolutionize the industry, reviving trust and providing a more transparent and safer environment.

The Blockchain-based Lottery System is the classic prototype of a secure lottery system built with blockchain technology. It employs the Bitcoin blockchain as a public random beacon for selecting winners and has an unpredictable and publicly observable process. It also employs a distributed-replicated ledger along with smart contracts to enable an open and secure system. Through open, query, subscribe, draw, check, and verify lottery services, the Blockchain-based Lottery System is a comprehensive and reliable means of holding lotteries.

The application of blockchain technology in the lottery industry has the potential to redefine the nature of lotteries as more transparent, secure, and credible. As technology advances, it will probably bring new and innovative lottery frameworks, further enhancing the players' experience and building confidence in the industry.

II. LITRATURE REVIEW

1) Blockchain-Based Lottery Systems for Securing Transparency

This particular study focuses on utilizing blockchain technology to improve trust concerns relating to centralized lottery systems. It discusses how blockchain, through its permanently fixed data and ability to be independently verified, can prevent fraudulent activities. The authors describe how each transaction related to ticket buying and prize distribution is publicly verifiable. It highlights the trustless execution of smart contract audits, consensus protocols, and permissioned participation.



2) Decentralized Lottery Systems Using Smart Contracts

This paper illustrates a model where the whole process of the lottery is encapsulated in smart contracts enabling execution without third party supervision. It discusses the Ethereum blockchain primarily because of its smart contract capabilities. The research elaborates on how contracts automate ticket sales, fund pooling, random drawing, and payout distribution. It also assesses gas costs relative to user interaction and proposes other measures such as batching transactions to optimize costs.

3) Cryptography and Blockchain Based Secure and Efficient Lottery Systems

Incorporating cryptographic protocols such as commitment schemes and verifiable secret sharing, this research focuses on fairness and security concerns of blockchain lotteries. The research describes the shortcomings of naïve pseudorandomness (e.g., block.timestamp) and introduces more robust mechanisms like zero-knowledge proofs and Chainlink VRF. It compares centralized vs decentralized randomness and explains how cryptographic audits reduce trust assumptions in the system.

4) Comprehensive Review of Blockchain-Integrated Lottery Systems

In studying the real-life cases of FairWin, PoolTogether, and LuckyBlock, this literature identifies gaps in contract drafting, gas expenditure, and randomness biasing. It classifies blockchain lotteries as no-loss deposit savings games and high-risk jackpots. This paper also evaluates usability issues, smart contract exploits, and suggests modular contract design with continuous monitoring as the primary maintenance strategy.

5) Enhancing Fairness and Security in Blockchain Lottery Systems

This paper underscores fairness by analyzing proof mechanisms such as Chainlink VRF and timestamp-independent entropy sources, investigating their impact on random number generation. It elaborates how results verification fosters user trust. Moreover, it incorporates game theoretical frameworks aimed at winner early disclosure, winner down-escrow, and front-running prevention. Decentralized gambling's legal and moral implications are examined as well.

6) Decentralized Lottery Systems Based On Ethereum Smart Contracts

This research explores the implementation of decentralized lottery systems on the Ethereum blockchain focusing on business issues such as transaction cost, scalability, and interoperability. It describes the use of Solidity for automation of basic procedures including ticket check, ETH payment, and automated drawing using Chainlink Keepers. It also discusses employing Layer-2 solutions (e.g. Optimism, Arbitrum) to optimize fees and enhance transaction throughput for universal access.

III. OBJECTIVES

1) In Pursuit of The Ensured Proper Conduct of the Lottery Process:

To guarantee fairness/balance and randomness, this Lottery System based on Blockchain Technology intend to utilize the Ethereum blockchain alongside the Isaac algorithm in conducting lotteries.

2) To Increase Overall Efficiency in Lottery Functions, Operational Workflows, and Customer Relations:

The goals emphasize on achieving performance, scalability, and usability by utilizing Ethereum smart contracts, layer 2 solutions, and updates in Ethereum 2.0 to enable smooth operations for users.

3) To Allow Users Participation Beyond Geographical Locations in the Lottery System:

The global decentralized nature of Ethereum can be leveraged in propelling the Blockchain-based Lottery System to improve the accessibility and inclusivity in the lottery system across users all over the world.

IV. METHODOLOGY

The idea here is to use blockchain technology to enhance the security, reliability, and transparency of lotteries. Blockchain is a special kind of digital record that keeps data safe from being changed, making it perfect for applications like lotteries. This platform includes: Blockchain (Distributed Ledger Technology), Cryptographic Concepts, Decentralized Consensus Protocols, and Smart Contracts. When these technologies come together, they ensure that the lottery process is transparent—everyone can see the rules and outcomes. It's fair (no one can tamper with it) and transparent (you can track the whole process from start to finish). The goal is to harness the trustworthiness of blockchain to create lotteries that are more dependable and free from fraud, all while integrating real-world user experiences into its learning process.

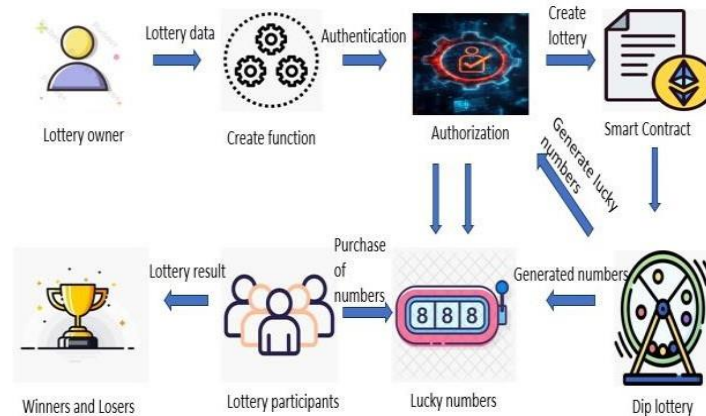


Fig 1. Process Flow

A. System Design and Architecture

1) System Planning and Requirement Analysis

a) When it comes to planning and analyzing requirements for a smart lottery system, it's all about pinpointing both the functional and non-functional needs. On the functional side, we're looking at essentials like user registration, wallet integration, ticket purchases through smart contracts, a fair way to select winners, and transparent prize distribution. Non-functional requirements, on the other hand, emphasize security, scalability, usability, and performance, ensuring the system can handle a lot of users while still being easy to navigate. Plus, we can't forget about compliance with legal regulations for online gambling and cryptocurrency use. By tackling these requirements head-on, we can build a system that prioritizes fairness, security, and a seamless user experience.

2) Architecture

a) The structural design of the system is crucial for the success of this project. It's all about creating a system that's easy to scale, flexible, and straightforward to update. This means carefully planning how data flows through the system, how its various components interact, and how it connects with any external services. The ultimate goal is to develop a system that can accommodate more users and features as it grows, while also being easy to maintain and enhance over time.

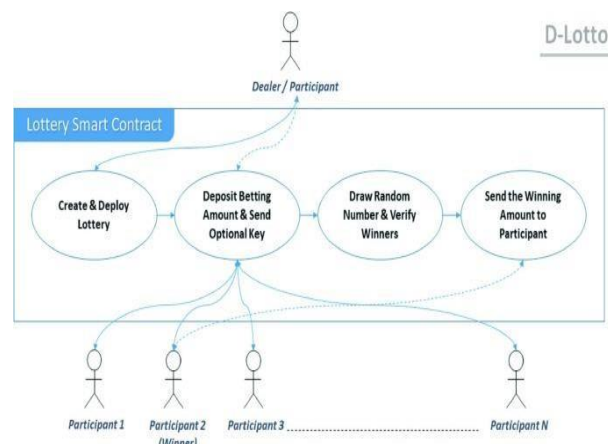


Fig 2. Architecture Design

3) Technologies

a) For a smart lottery system, the tech stack includes Ethereum as the blockchain platform, ensuring security and transparency. We use Solidity for crafting smart contracts, while the frontend is designed with HTML, CSS, and Node.js, and the backend is powered by Solidity and web3.js.

NLP: For chatbots or help systems, consider Hugging Face, spaCy, or NLTK.

B. Version Control & APIs

Use GitHub or GitLab, along with Etherscan and Chainlink; optional analytics or OpenAI APIs can be handy too.



- C. Other Requirements
1. Data - You'll need lottery history, smart contract logs, and user analytics.
 2. Connectivity - A reliable internet connection and node access (via Infura or Alchemy) are essential.
 3. UI/UX - Make sure to integrate a Web3 wallet, provide live results, allow ticket downloads in PDF format, and ensure a responsive design with dark mode.
 4. Authentication - Implement Web3 login or email/OTP, and set up role-based access for Admin, User, and Auditor.

V. CONCLUSION

This paper presents an innovative approach that leverages the Ethereum network for buying and selling lottery tickets. By implementing this system, we aim to overhaul traditional lottery operations entirely—eliminating the need for third parties during the purchasing process, streamlining how prizes are declared, and simplifying the prize claiming process. The winning numbers will be generated using our proposed random number generator. Every transaction will be recorded on the blockchain, along with the prize details, creating a transparent and verifiable system for all participants. Overall, this new system addresses nearly all the major issues associated with traditional lotteries, ensuring fairness for consumers in the process.

REFERENCES

- [1]. <https://ieeexplore.ieee.org/document/9997830>
- [2]. <https://ieeexplore.ieee.org/document/10489454>
- [3]. <https://ieeexplore.ieee.org/document/10266035>
- [4]. https://www.researchgate.net/publication/338370062_BanFEL_A_Blockchain_Based_Smart_Contract_for_Fair_and_Efficient_Lottery_Scheme
- [5]. <https://www.ijraset.com/research-paper/secured-lottery-system-using-smart-contract-and-blockchain-technology>