Decentralized Lottery System

CS411 - Blockchain Project

Group Members

Hamza Hasan - 2021197

M Zulfiqar Ali - 2021

Problem Statement

Problem Statement:

Traditional raffle systems often face challenges such as:

- **Lack of Transparency:** Users cannot verify the fairness of ticket handling or winner selection.
- **Centralized Control:** Dependence on a central authority increases the risk of manipulation or fraud.
- **Limited Security:** Potential vulnerabilities in funds management and data privacy.

Objective:

- **Decentralization:** Eliminate the need for intermediaries by using blockchain technology to facilitate transparent, secure raffle operations.
- **Security and Transparency:** Ensure fairness in ticket purchases, winner selection, and prize distribution through immutable smart contracts.
- **Random Winner Selection:** Use a pseudo-random algorithm to select a winner in a transparent and fair manner, verifiable on the blockchain.
- **Secure Fund Withdrawal:** Allow the winner to withdraw collected Ether securely once the raffle is concluded.

Project Overview

What is Lottery DApp?

- A decentralized application allowing users to participate in a lottery by sending 0.1 ETH.
- Manager can pick a winner, who can then claim the prize.

Key Features:

- Secure and transparent transactions.
- Manager-controlled winner selection.
- User-friendly interface with MetaMask integration.

System Architecture

Components

- **Smart Contract:** Manages lottery logic on the blockchain.
- **Frontend (React):** User interface for interacting with the DApp.
- **Blockchain Network:** Ethereum (local Hardhat network).

Interaction Flow

- Users interact via the frontend, which communicates with the smart contract through Ethers.js.

Smart Contract

Overview: Written in Solidity, deployed using Hardhat.
Key Functions:
- enter(): Allows users to enter the lottery.
- pickWinner(): Manager picks a random winner.
- claimPrize(): Winner claims the prize.

Security Measures:
- onlyManager modifier to restrict access.
- Re-entrancy protection via proper state updates.

Frontend

Technologies Used:

- React: For building the user interface.
- Ethers.js v6: For blockchain interactions.
- React Router: For navigation between pages.

User Features:

- Entering the lottery.
- Picking a winner (manager only).
- Claiming prizes.

Design Considerations:

- Responsive design for various devices.
- Clear status indicators and user feedback.

Conclusion

- Successfully developed and deployed a functional Lottery DApp.
- Ensured security and performance through rigorous testing.
- Created a user-friendly interface facilitating seamless interactions.

Impact: Demonstrated the potential of blockchain for creating transparent and secure lottery systems.

Next Steps: Implement planned enhancements to elevate the DApp to production-ready standards.