BPWHF END-SEM PROJECT
LOTTERY DAPP

Supervised By: Prof./Dr. Shahid Afridi Saikia

Section: 34
Group No: 11
Name of the Student(s) with Regd. No.:
Name-Riya Ram (2241018048)
Name-Aishika Chakraborty(2241003004)
Name-Pallavi Meher(2241013107)
Name-Anwesha Mishra(2241013126)

Department of Computer Science and Engineering
Faculty of Engineering & Technology (ITER)
Siksha 'O' Anusandhan (Deemed to be) University
Bhubaneswar, Odisha

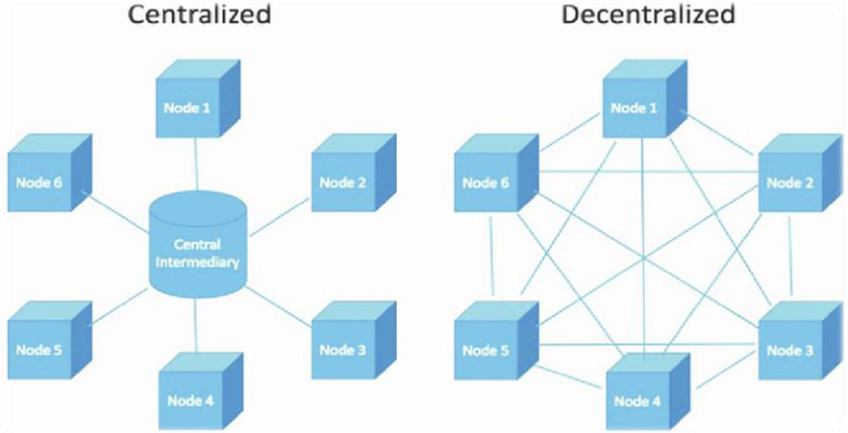
Introduction

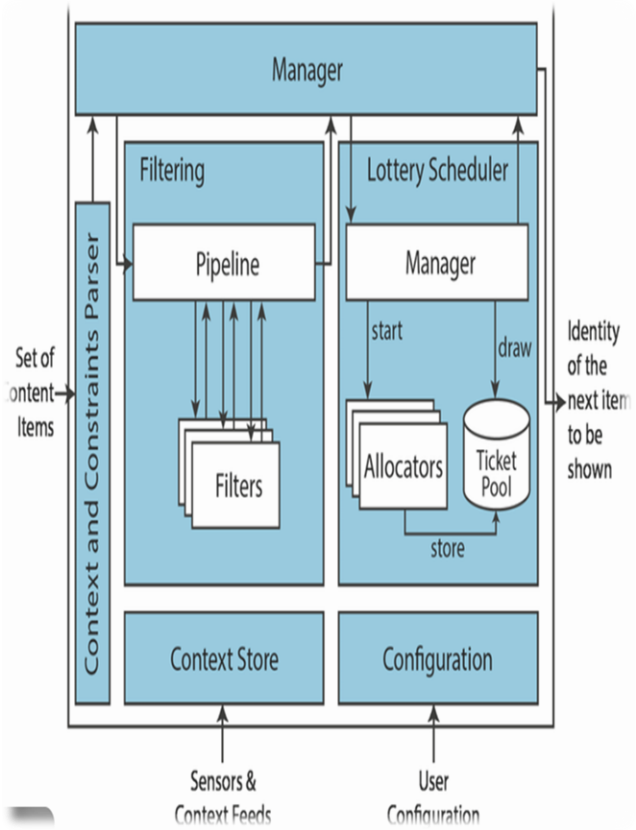
=>The Lottery Decentralised Application (Lottery DApp) is a blockchain-based system developed with the primary objective of creating a tamper-proof, trustless, and fully automated lottery platform without the involvement of any intermediary or central authority. In traditional lottery systems, a third party is responsible for managing ticket sales, selecting winners, and distributing prizes, which introduces risks related to data manipulation, unfair practices, and a lack of transparency.

=>To eliminate these issues, this project utilises blockchain technology and smart contracts to ensure that all lottery operations are executed automatically and securely. The smart contract acts as the sole authority of the system, enforcing predefined rules for participant registration, fund collection, winner selection, and prize distribution. Once deployed, the contract code cannot be altered, making the system tamper-proof and resistant to manipulation.

=>The system is designed to operate without any man-in-the-middle handling, as users directly interact with the smart contract through a decentralised frontend and a cryptocurrency wallet. All transactions are recorded on the blockchain, providing immutability, transparency, and public verifiability. This project demonstrates how decentralised applications can replace trust in intermediaries with trust in code.

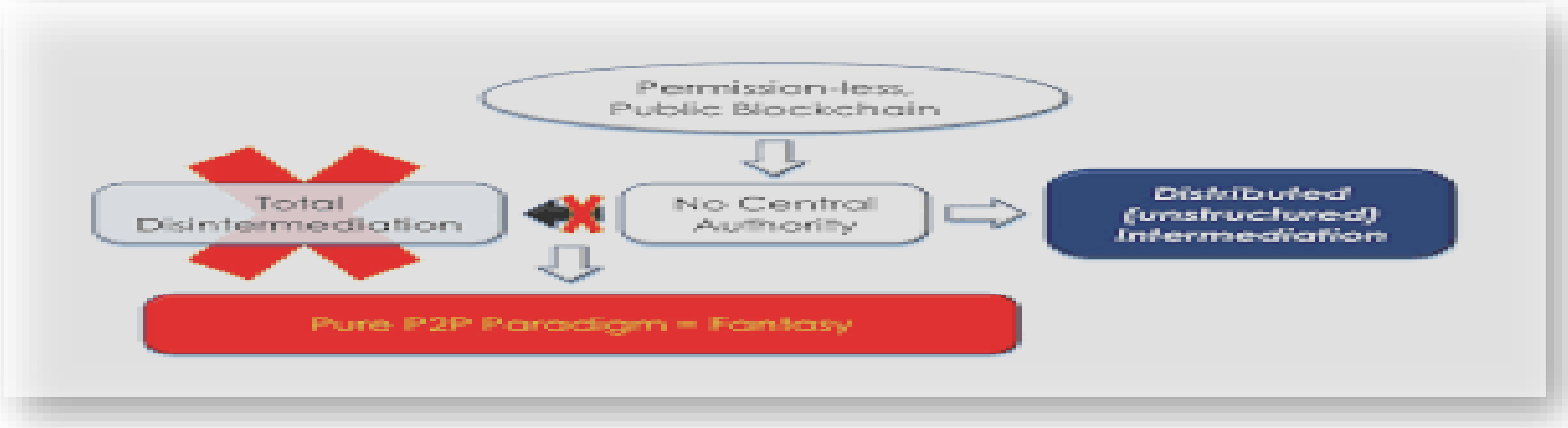
Traditional lottery systems operate under centralized control, requiring participants to trust intermediaries for ticket management, winner selection, and prize distribution. This dependence on a central authority introduces risks such as a lack of transparency, potential manipulation, and man-in-the-middle handling of funds and data. To address these issues, our project is motivated by the need for a tamper-proof and trustless lottery system where human intervention is eliminated. By leveraging blockchain technology and smart contracts, all lottery rules are enforced automatically and cannot be altered once deployed. This ensures transparency, security, and fairness, allowing users to directly interact with the system without relying on any intermediary.



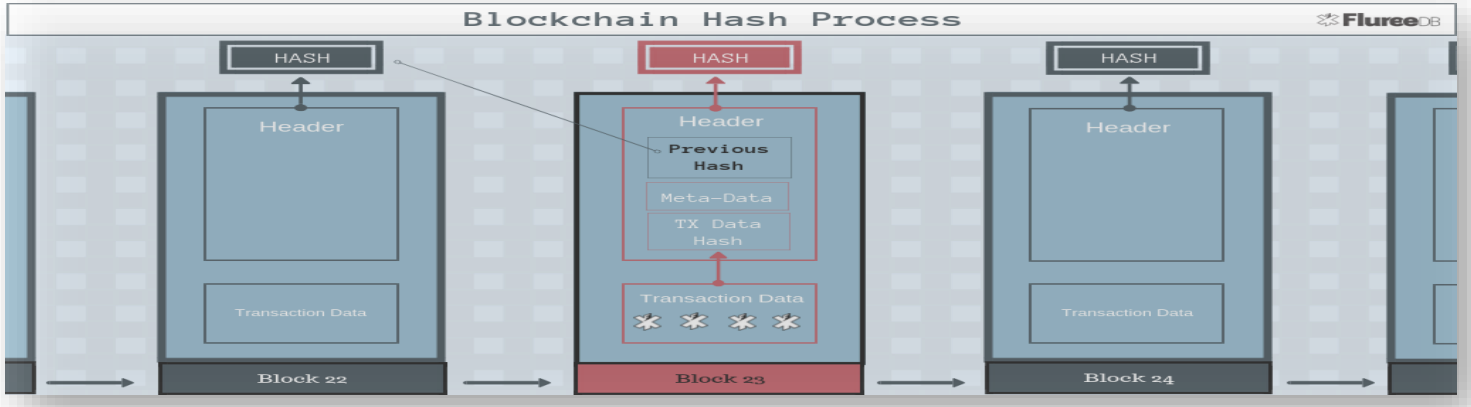


How unique is our decentralised application?

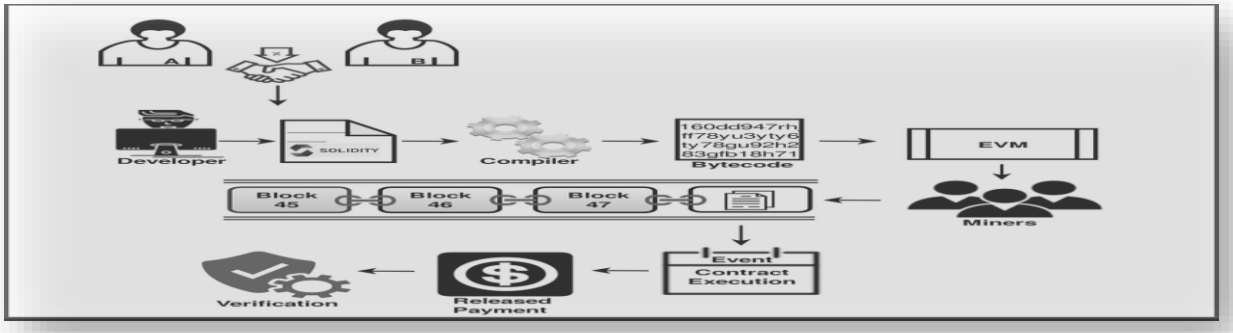
1. Our system removes man-in-the-middle handling by allowing direct blockchain interaction



2. Tamper-Proof Smart Contract

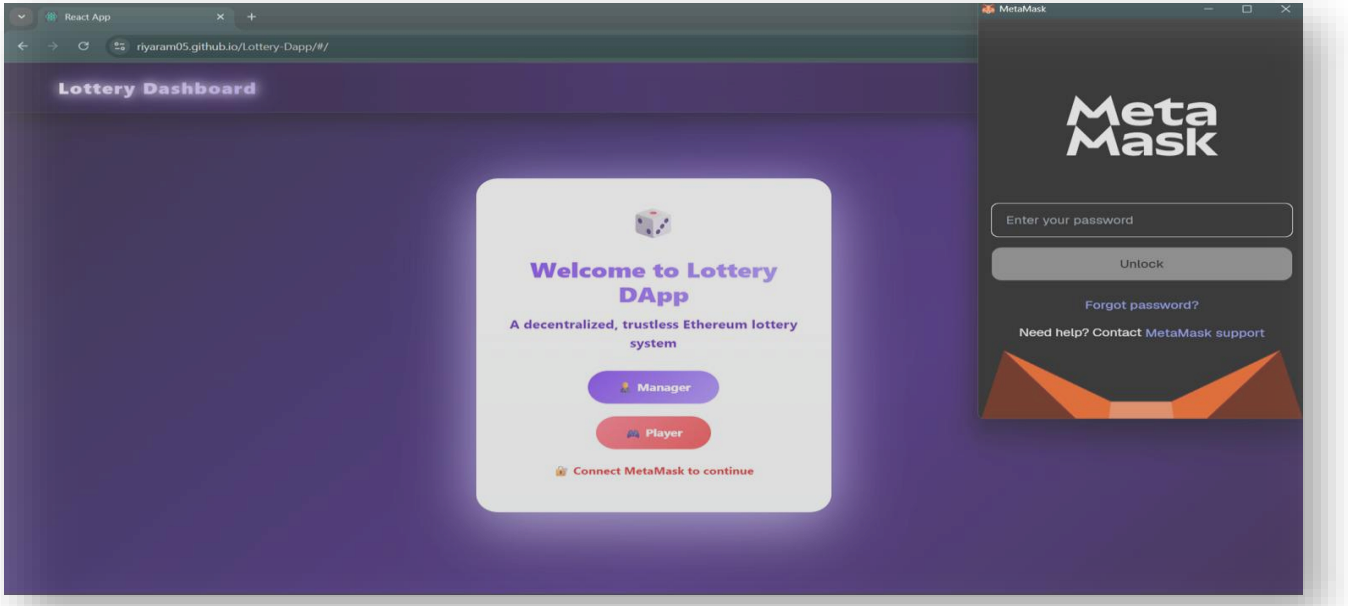


3. Automation Using Smart Contracts

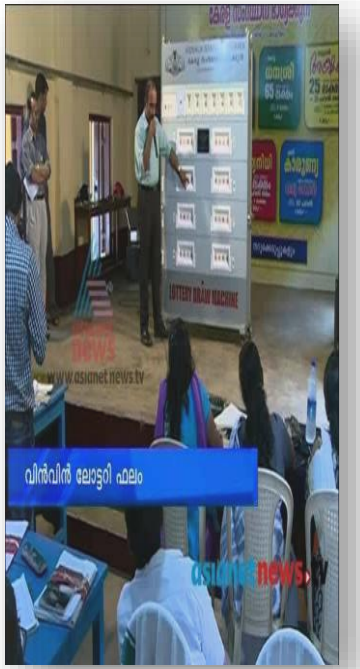


4. Every Transaction is publicly verifiable

5. Wallet authentication, which ensures secure and permissionless access



Literature Survey

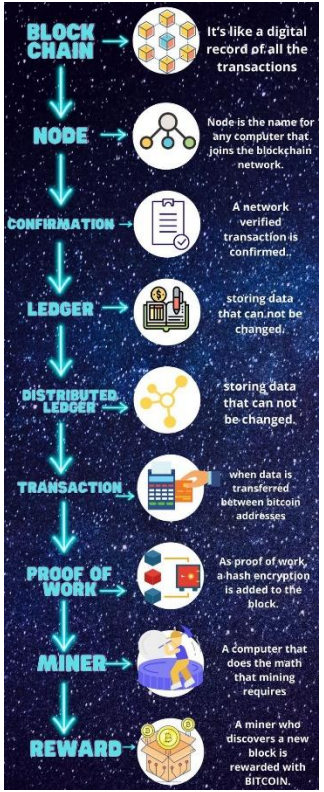


(i) Existing System

- Traditional lottery systems are centralized
- Controlled by government or private organizations
- Ticket sales, winner selection, and prize distribution are manually managed
- Users must trust the authority for fairness
- Limited transparency and delayed payouts

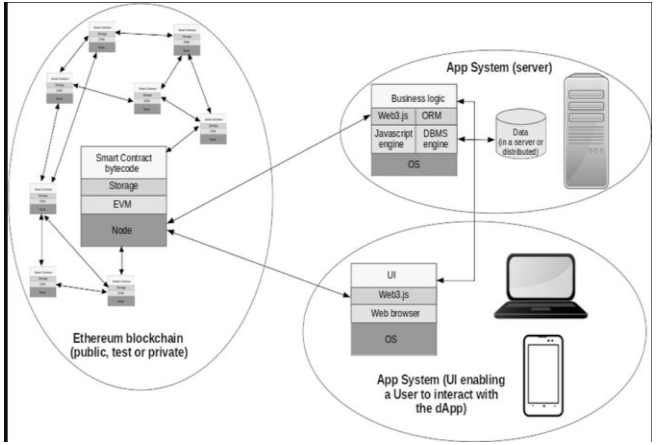
(ii) Identifying the problem

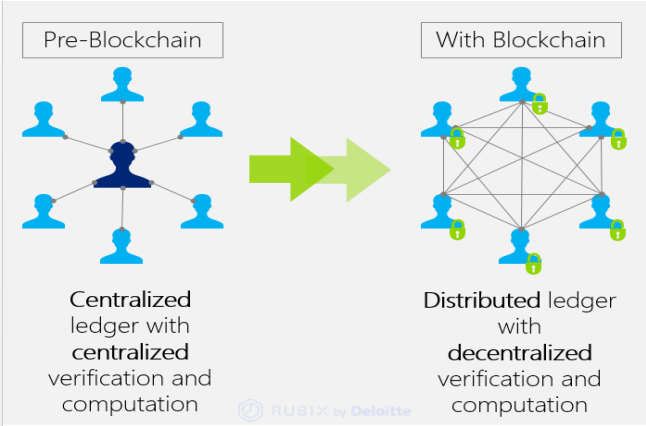
Traditional lottery systems operate under centralized control, where all critical processes such as ticket sales, winner selection, and prize distribution are managed by a single authority. This centralized architecture introduces several challenges, including lack of transparency, as participants cannot independently verify the fairness of the lottery process. The presence of intermediaries creates a man-in-the-middle scenario, increasing the risk of manipulation, fraud, and misuse of funds. Additionally, centralized systems suffer from single points of failure, making them vulnerable to system outages or malicious attacks. Delayed prize distribution and limited auditability further reduce user trust. These issues highlight the need for a secure, tamper-proof, and trustless lottery system that eliminates human intervention and ensures transparent and automated execution.



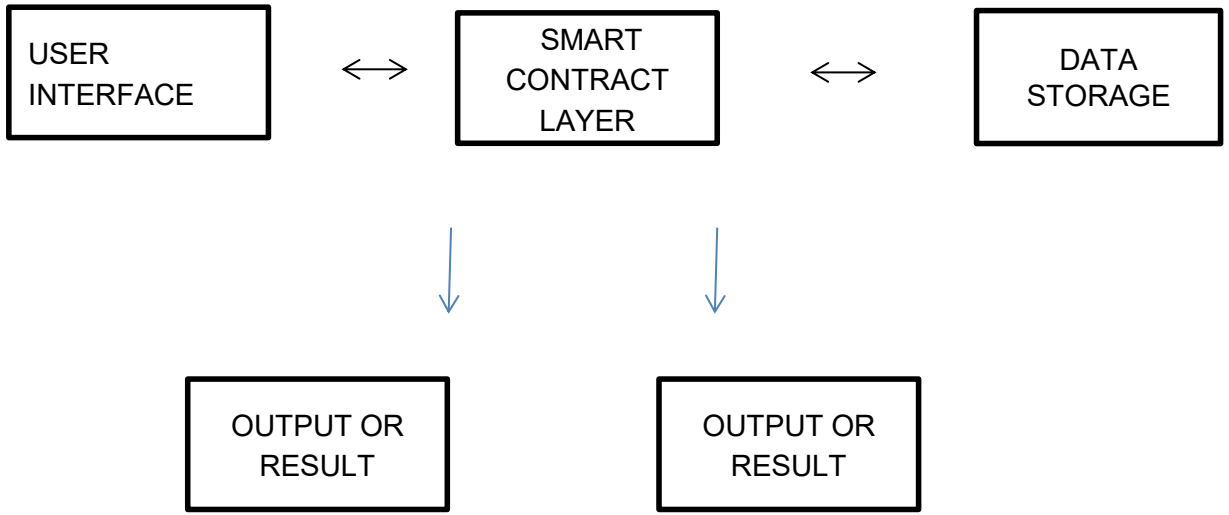
(iii) Architecture of the project

=> The Lottery DApp employs a decentralised architecture that eliminates intermediaries and ensures tamper-proof execution. The system consists of four main components: Frontend Interface, Smart Contract, Blockchain Network, and Wallet Integration.
=> The frontend provides a user-friendly interface through which participants interact with the system. Users connect their cryptocurrency wallet to enter the lottery. All lottery logic, including participant registration, fund collection, random winner selection, and prize distribution, is implemented inside a Solidity smart contract deployed on the blockchain.
=> The blockchain network ensures immutability, transparency, and security by permanently recording all transactions. Wallet integration enables secure authentication and transaction signing, allowing users to interact directly with the smart contract without any man-in-the-middle involvement. This architecture ensures automated, trustless, and transparent lottery operations





Schematic Layout



Tools And Algorithms

Methods
- Smart contract-based automation
- Decentralised fund handling
- Wallet-based authentication

Tools
- Solidity (Smart contracts)
- Remix IDE
- MetaMask
- React.js
- Web3.js

Algorithm

•Deploy the smart contract and assign the deployer as manager.
•Participants enter the lottery by sending 1 Ether to the contract.
•Valid participant addresses are stored on the blockchain.
•A pseudo-random number is generated using blockchain parameters.
• The manager selects the winner when at least 3 participants join.
• The winner is chosen using the modulo operation and receives the total balance.
•Participant list is reset for the next lottery round.

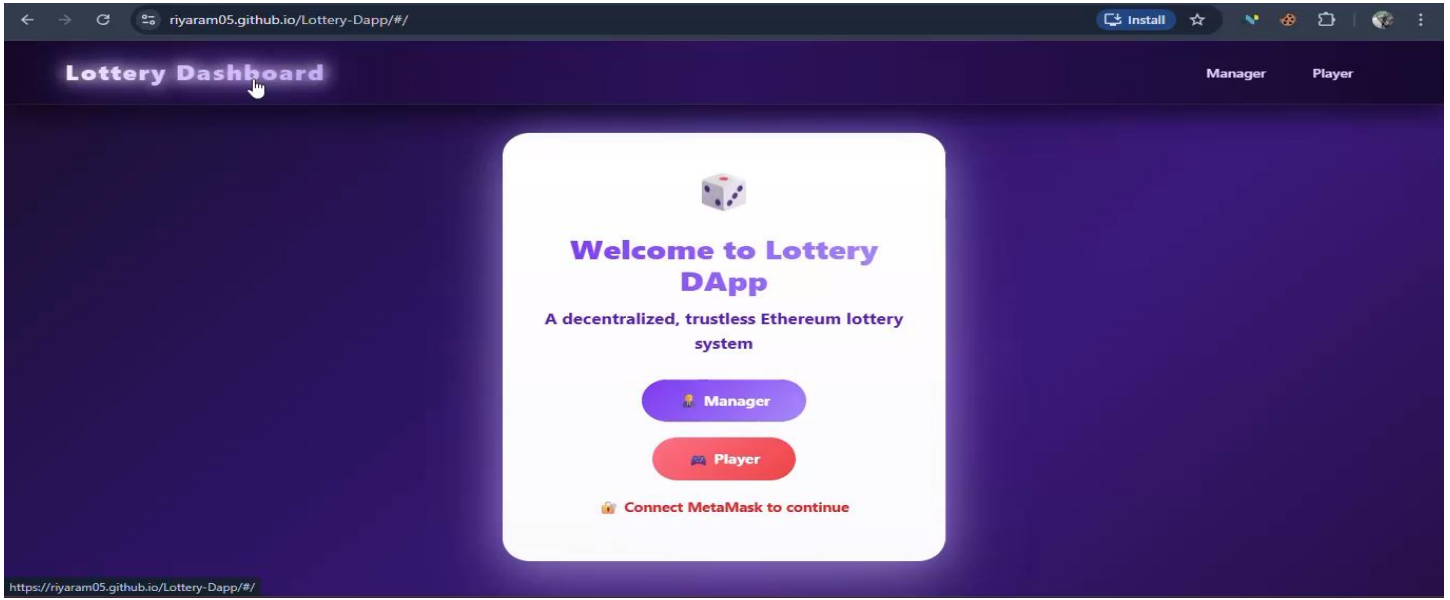
Experimentation and Results

System Specifications

Hardware Requirements
Processor: Intel i3 / Ryzen 3 or above
RAM: Minimum 8 GB
Storage: 256 GB SSD or above
Software Requirements
Operating System: Windows / Linux
Browser: Google Chrome / Brave
Blockchain Wallet: MetaMask
IDE: Remix IDE, VS Code
Blockchain & Tools
Smart Contract Language: Solidity
Blockchain Network: Sepolia Testnet
Frontend: HTML, CSS, React.js
Libraries: Web3.js

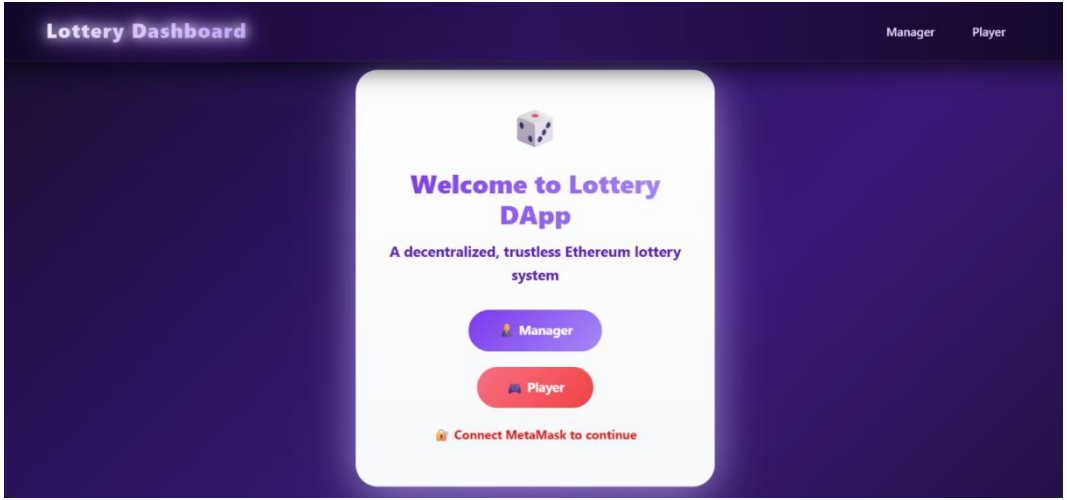
Experimentation and Results

The frontend of the application is hosted online at https://riyaram05.github.io/Lottery-Dapp

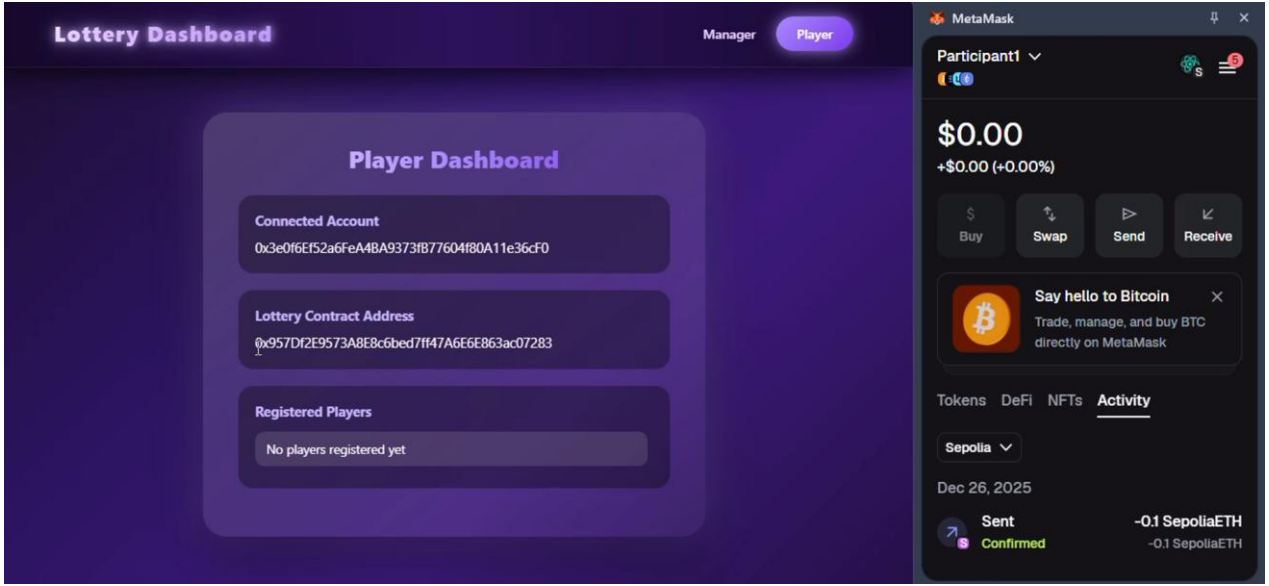


ScreenShots

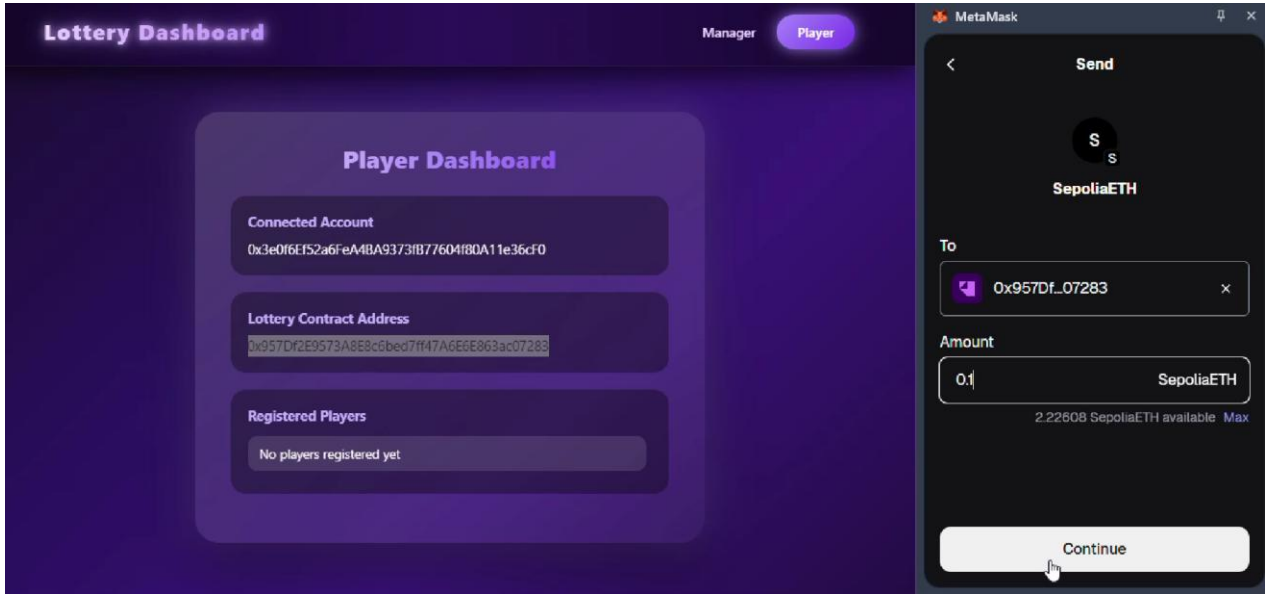
a. Homepage / Lottery Page :- Displays the lottery interface and current lottery status.



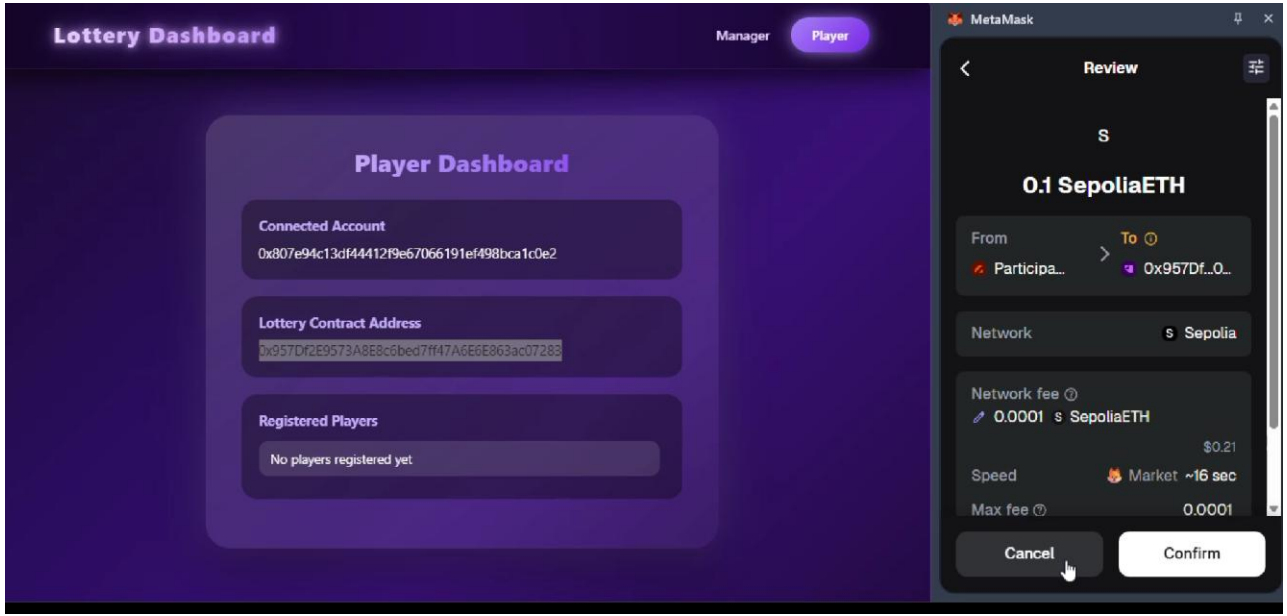
- **b. Wallet Connection :-**User connects MetaMask wallet to interact with the Lottery DApp



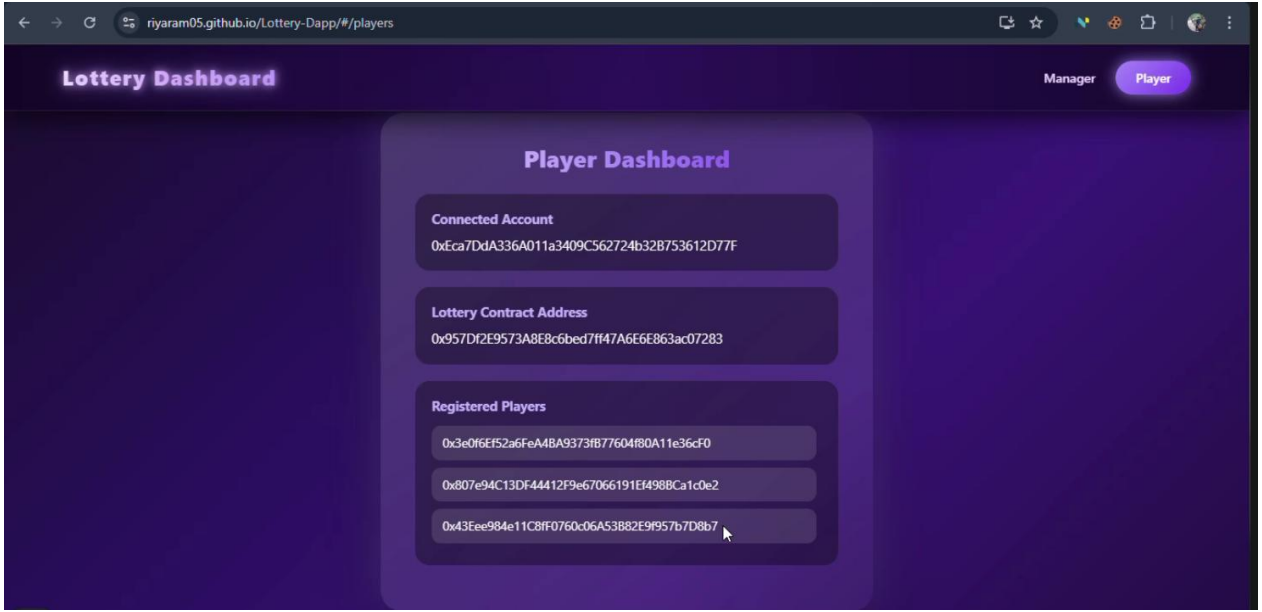
- **c. Lottery / Ticket Purchase :-**User enters the lottery by sending Ether (ETH) to the smart contract.



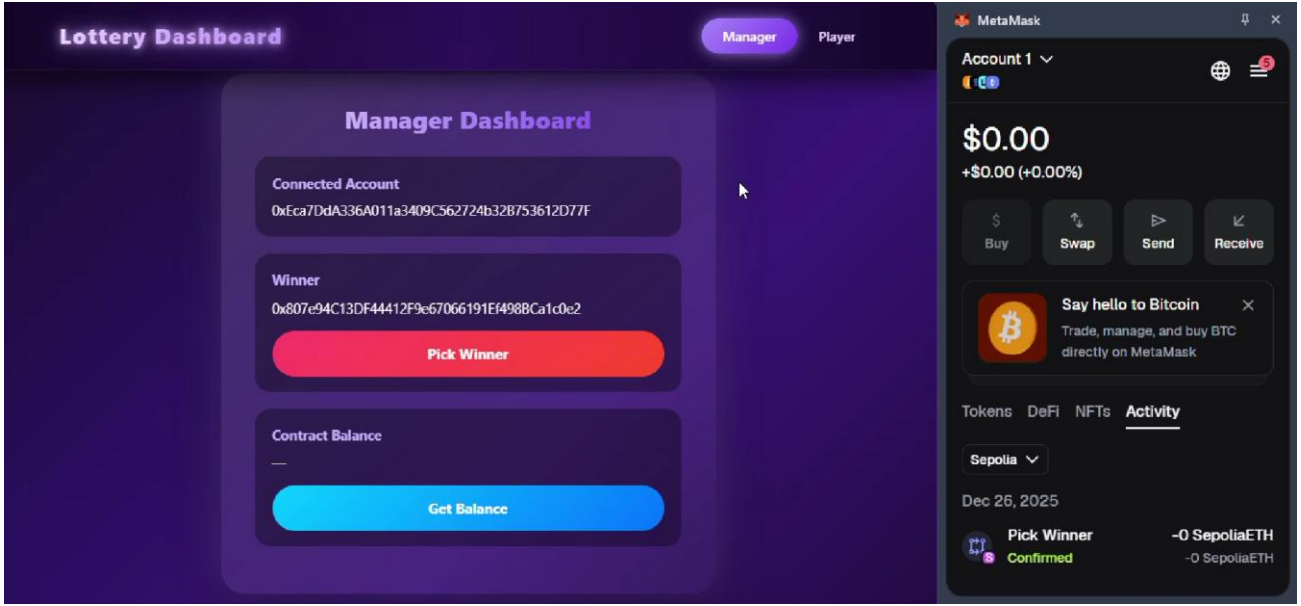
- **d. Transaction Confirmation :-**Ethereum transaction is securely validated and recorded on the blockchain.



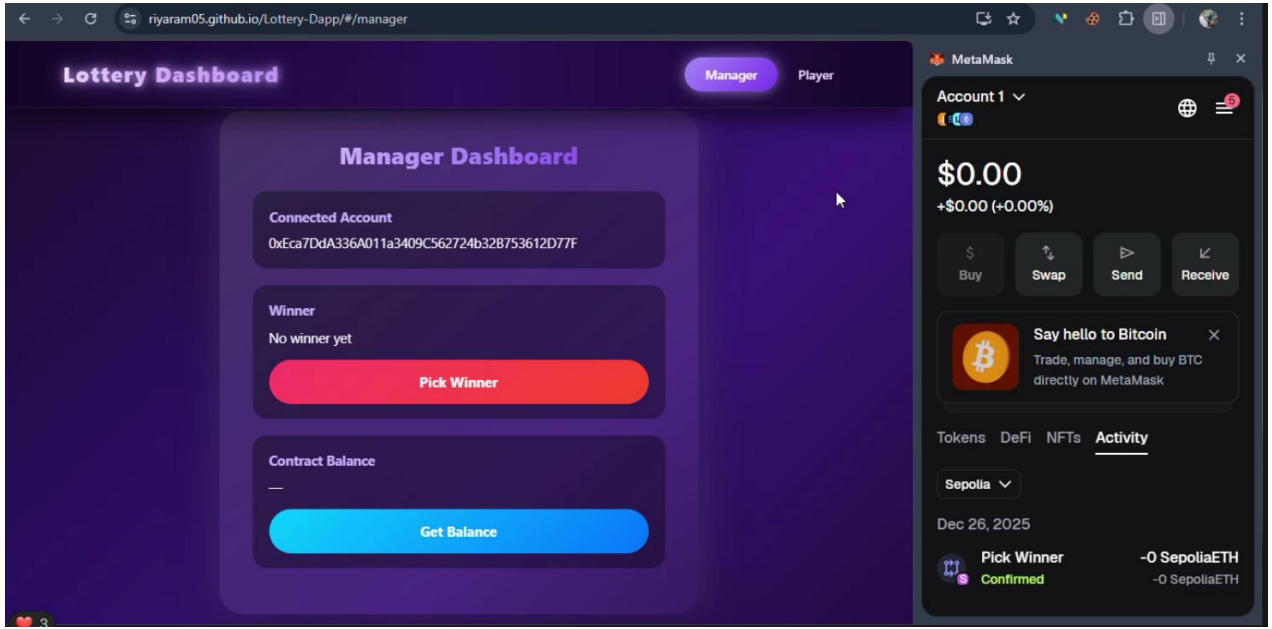
- **e. Participant Registration :-**Participant address is automatically stored in the Ethereum smart contract .



- **f. Winner Selection :-**Smart contract executes automated winner selection on Ethereum.



- **g. Prize Distribution :-**Ether (ETH) is transferred directly to the winner’s wallet.



Conclusion and Future Scope

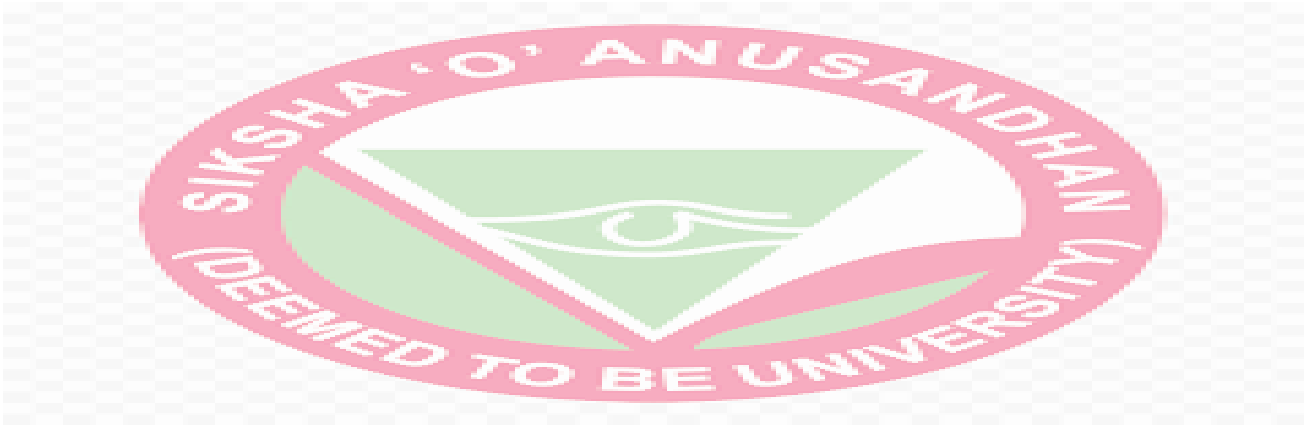
•The proposed Lottery DApp is more efficient than traditional lottery systems due to full automation using smart contracts.
•It eliminates manual processing and third-party involvement, reducing time delays and operational overhead.
•Winner selection and prize distribution are executed instantly on the Ethereum blockchain.
•The decentralized architecture ensures faster execution, higher security, and greater transparency.
•Overall, the system provides a more reliable, scalable, and efficient solution compared to existing centralized lottery systems.

Future Scopes

- Can be deployed on multiple blockchain networks.
- More secure random winner selection can be implemented.
- Support for different types of lotteries can be added.
- User interface can be improved for mobile devices.
- System can be extended to other decentralized applications.

Bibliography

[1] S. Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System,"* 2008. [Online].
Available:https://bitcoin.org/bitcoin.pdf
[2] G. Wood, *"Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper),"* 2014.
[Online].
Available: https://ethereum.github.io/yellowpaper/paper.pdf
[3] Ethereum Foundation, *"Ethereum Official Documentation."* [Online].
Available: https://ethereum.org/en/developers/docs/
[4] Solidity Developers, *"Solidity Official Documentation."* [Online].
Available: https://docs.soliditylang.org/
[5] MetaMask, *"MetaMask Developer Documentation."* [Online].
Available: https://docs.metamask.io/
[6] Web3.js & Ethers.js, *"Official Library Documentation."* [Online].
Available:https://web3js.readthedocs.io/ , https://docs.ethers.org/



Thank You