INDEX

1. INTRODUCTION

Lotteries have been a popular form of gambling and fundraising for centuries, providing entertainment and generating funds for various causes. However, traditional lottery systems suffer from several issues, including **lack of transparency, high operational costs, fraud risks, slow payouts, and limited accessibility**. These problems arise primarily due to the reliance on centralized authorities, which control ticket sales, winner selection, and fund distribution. Participants must blindly trust these entities, even though cases of mismanagement, unfair practices, and corruption have been reported worldwide.

With the rise of **blockchain technology and smart contracts**, a new decentralized lottery model is emerging, addressing these challenges by ensuring **transparency, security, automation, and fairness**. Blockchain-based lotteries operate on **immutable and publicly verifiable ledgers**, eliminating the need for intermediaries. Every transaction, from ticket purchases to prize distributions, is recorded transparently, making fraud and manipulation nearly impossible. Smart contracts, which are self-executing programs on the blockchain, automate lottery operations by enforcing predefined rules, ensuring that the process is fair and tamper-proof.

One of the key advantages of blockchain-based lotteries is **provably fair randomness**. In traditional systems, random number generation (RNG) mechanisms are often opaque, raising concerns about biased or rigged results. Blockchain lotteries use **verifiable random number generators (RNGs)** such as **Chainlink VRF**, which provide cryptographic proof that the selection process is truly random and cannot be altered. This guarantees that every participant has an equal chance of winning.

2.BACKGROUND

Traditional lottery systems often face challenges related to **trust, transparency, and efficiency**. Many centralized lotteries suffer from **manipulation, high operational costs, slow payouts, and lack of public verification**. Participants must trust the organizers to conduct fair draws and distribute winnings correctly, which can lead to fraud or mismanagement.:

2.1 Trust Issues in Traditional Lotteries

Traditional lotteries require users to trust centralized entities to manage funds and ensure fairness.

However, cases of fraud, mismanagement, and lack of transparency have raised concerns. Players have no way to verify if the lottery is being conducted fairly or manipulated. This creates a **trust gap**, discouraging participants from engaging in such systems. Blockchain-based lotteries aim to eliminate this **trust dependency** through decentralization.

2.2 Lack of Transparency

Traditional lottery operations are not fully **open for public verification**. The winner selection process, fund allocation, and ticket tracking often remain hidden. This lack of transparency increases the risk of **fraud and manipulation** by centralized authorities.

Participants must blindly trust the system, without proof of a fair process. Blockchain ensures **public and immutable record-keeping**, making lotteries fully transparent.

2.3 High Operational Cost

Centralized lotteries involve **middlemen, administrative expenses, and infrastructure costs**.

These costs reduce the total prize pool, meaning participants receive less in winnings.

Advertising, commissions, and regulatory compliance further increase expenses. A blockchain-based lottery **eliminates intermediaries**, reducing unnecessary costs. More funds remain within the system, leading to **higher payouts** for winners.

2.4 Slow Payouts

In traditional lotteries, winners often experience **delays in receiving their prizes**. This is due to manual verification, legal processes, and bank transaction delays. Such inefficiencies create frustration and reduce trust in the system. Smart contracts enable **instant and automated payouts** to winners. Funds are transferred directly to the winner's wallet **without human intervention**

2.5 Smart Contracts for Automation

Smart contracts **automate key lottery functions**, reducing the need for intermediaries. Ticket validation, winner selection, and prize distribution occur without manual interference. Once predefined conditions are met, the contract executes autonomously. This eliminates human error and ensures the process follows **predefined rules**. As a result, lotteries become **faster, fairer, and more efficient**.

3.BLOCKCHAIN BASICS

Blockchain technology is revolutionizing online marketplaces by offering transparency, security, and decentralization. Traditional marketplaces rely on intermediaries for transactions, which can introduce inefficiencies and high costs. Blockchain eliminates the need for third-party oversight, ensuring a more trustless, efficient system. Below are key blockchain concepts relevant to marketplace applications.

3.1 Decentralization

- In a decentralized marketplace, users transact directly with one another without a central authority controlling platform [1].
- This reduces dependency on intermediaries, lowering transaction costs and increasing system reliability [1].
- Peer-to-peer (P2P) networks in decentralized marketplaces ensure uninterrupted access even if a central server fails.

3.1 Immutability

- Immutability means that once data is recorded in the blockchain, it cannot be altered or deleted. This ensures transaction records remain tamper-proof, enhancing buyer and seller trust [2].
- .In the marketplace, order histories, product authenticity, and user reviews stored on a blockchain remain permanent and verifiable [2].

3.2 Smart Contracts

Smart contracts are self-executing contracts with predefined rules coded into them.

3.3 Key Components of Blockchain

1. **Blocks**: **Blocks**: Each block contains transaction details, a timestamp, and a reference (hash) to the previous block, ensuring a secure transaction history [1].
2. **Consensus Mechanisms**: Marketplaces use consensus protocols like Proof of Stake (PoS) to validate transactions and prevent fraud [2].
    - **Proof of Work (PoW)**: Used in Bitcoin but is energy intensive.
    - **Proof of Stake (PoS)**: More efficient and widely adopted in modern blockchain networks like Ethereum 2.0 [3].
    - **Delegated Proof of Stake (DPoS)**: Allows users to vote for delegates who validate transactions, improving scalability.
    - **Byzantine Fault Tolerance (BFT)**: Ensures security in decentralized networks by allowing consensus even with some malicious actors.
3. **Tokens**: Many blockchain marketplaces use native tokens for payments, rewards, or governance. These can be fungible (cryptocurrencies) or non-fungible tokens (NFTs) [3].
4. **Public and Private Keys**: Transactions require cryptographic keys, public keys act as user addresses, while private keys provide security and control over assets [2].

3.4 Key Advantages of Blockchain Technology

1. **Trust and Transparency:** Transactions recorded on a public ledger prevent data manipulation and fraudulent activities [1].
2. **Lower Fees:** Eliminating intermediaries significantly reduces processing fees, benefiting both buyers and sellers [2].
3. **Security:** Cryptographic hashing and decentralization make blockchain marketplaces highly resistant to hacks and fraud [3].
4. **Ownership and Provenance**: NFTs on blockchain marketplaces allow digital

goods (e.g., art, collectibles, and virtual assets) to be uniquely owned and traded with verified authenticity [3].

5. **Enhanced Payment Options**: Cryptocurrency transactions enable cross-border payments with minimal fees and faster processing times.

Use Cases of Blockchain in Marketplaces

- **E-commerce:** Decentralized marketplaces enable peer-to-peer product sales without relying on centralized platforms like Amazon or eBay [1].
- **NFT Marketplaces**: Platforms like OpenSea and Rarible allow users to buy, sell, and trade digital collectibles and artwork using blockchain [2].
- **Freelancing Platforms:** Blockchain-powered gig economy platforms enable direct transactions between freelancers and clients, reducing commission fees [3].
- **Supply Chain Marketplaces**: Blockchain enhances transparency in product sourcing and supply chain management.
- **Gaming Marketplaces**: Play-to-earn and blockchain-based gaming economies allow players to trade in-game assets securely.
- **Content Monetization**: Blockchain allows content creators to receive direct payments from consumers without intermediaries.
- **Real Estate:** Tokenized property ownership and smart contract-based transactions simplify property buying and selling [2].

4 USE CASE OVERVIEW

A blockchain-based lottery smart contract offers a transparent, decentralized, and secure alternative to traditional lotteries. Users purchase lottery tickets using **cryptocurrency**, and the smart contract autonomously records transactions, ensuring fairness. A provably fair random number generator (**RNG)** selects winners, eliminating fraud or manipulation.

The system ensures **instant payouts**, with winnings automatically transferred to the winner's wallet, reducing reliance on intermediaries. **Privacy** is enhanced through zero-knowledge proofs and stealth addresses, ensuring user anonymity. The lottery's immutable blockchain ledger allows for **public verification**, preventing disputes.

This system benefits from **lower operational costs**, **global accessibility**, and **high security** due to blockchain's tamper-proof nature. Additionally, it can integrate **regulatory compliance** features like **KYC/AML** if required. The use case applies to national lotteries, charity raffles, decentralized gaming, and community-driven fundraising, providing a **fair and efficient** lottery system.

4.1 Objectives

Here are **objectives** for a blockchain-based lottery system:

1. **Transparency and Fairness**: Blockchain ensures all transactions are publicly recorded and verifiable, eliminating the risk of fraud. The random winner selection process is transparent and auditable.
2. **Decentralization**: The lottery is governed by smart contracts, eliminating the need for a central authority or intermediary. This ensures a trustless and autonomous system where no single party controls the process.
3. **Security**: Blockchain's cryptographic nature secures transactions and lottery results. Participants' funds and data are protected from fraud and manipulation.
4. **Automation and Efficiency**: Smart contracts automatically handle all aspects of the lottery, from ticket sales to prize distribution, reducing operational costs and delays. This ensures smooth and fast execution.

5. **Global Accessibility**: Participants from anywhere can enter the lottery using cryptocurrencies, making it a global and borderless system. This provides equal opportunity for people across different regions to participate.

4.2 Scope

Here are **5 scope points** for a blockchain-based lottery system:

1. **Global Participation**: The system allows users from any part of the world to participate, provided they have an internet connection and cryptocurrency wallet. This increases the reach and inclusivity of the lottery.
2. **Automated Prize Distribution**: The smart contract automatically distributes the prize to the winner's wallet, ensuring fast and accurate payouts without human intervention.
3. **Global Participation**: The system allows users from any part of the world to participate, provided they have an internet connection and cryptocurrency wallet. This increases the reach and inclusivity of the lottery.
4. **Automated Prize Distribution**: The smart contract automatically distributes the prize to the winner's wallet, ensuring fast and accurate payouts without human intervention.
5. **Transparent and Auditable Process**: Every transaction and lottery result is recorded on the blockchain, providing a fully transparent and auditable system for participants to verify the fairness.

4.3 Stakeholders

Here are the **stakeholders** involved in a blockchain-based lottery system:

1. **Participants (Users)**: Individuals who purchase lottery tickets and participate in the lottery. They expect a secure, fair, and transparent system for entering the lottery and claiming their rewards.

2. **Smart Contract (Lottery Contract)**: The autonomous code that governs the lottery process, including ticket sales, winner selection, and prize distribution. It ensures transparency, fairness, and automation in the system.
3. **Lottery Organizer/Developer**: Entities or developers who create, deploy, and manage the smart contract and the lottery platform. They are responsible for setting rules, monitoring the system, and ensuring its smooth operation.
4. **Regulatory Authorities**: Government bodies or legal institutions that may regulate or oversee the lottery system, ensuring it adheres to legal and ethical standards, especially in jurisdictions with gambling laws.
5. **Blockchain Network Providers**: Entities or platforms that provide the infrastructure for running the blockchain network (e.g., Ethereum, Binance Smart Chain

4.4Architecture

Here's the **architecture of a blockchain-based lottery system** :

4.4.1 User Interface (UI)

Provides an interface for participants to interact with the system.

Allows users to purchase tickets, check results, and claim rewards.

4.4.2 Blockchain Network

The decentralized infrastructure where data and transactions are stored.

Provides the security, transparency, and immutability for the entire system.

4.4.3 Smart Contract (Lottery Contract)

Automates the lottery process, including ticket purchases and prize distribution.

Ensures fairness and transparency by governing the lottery rules on the Blockchain.

4.4.4 Random Number Generation (RNG)

Ensures fairness by selecting the winner through a verifiable, random process.

Uses on-chain or decentralized oracle services like **Chainlink VRF**

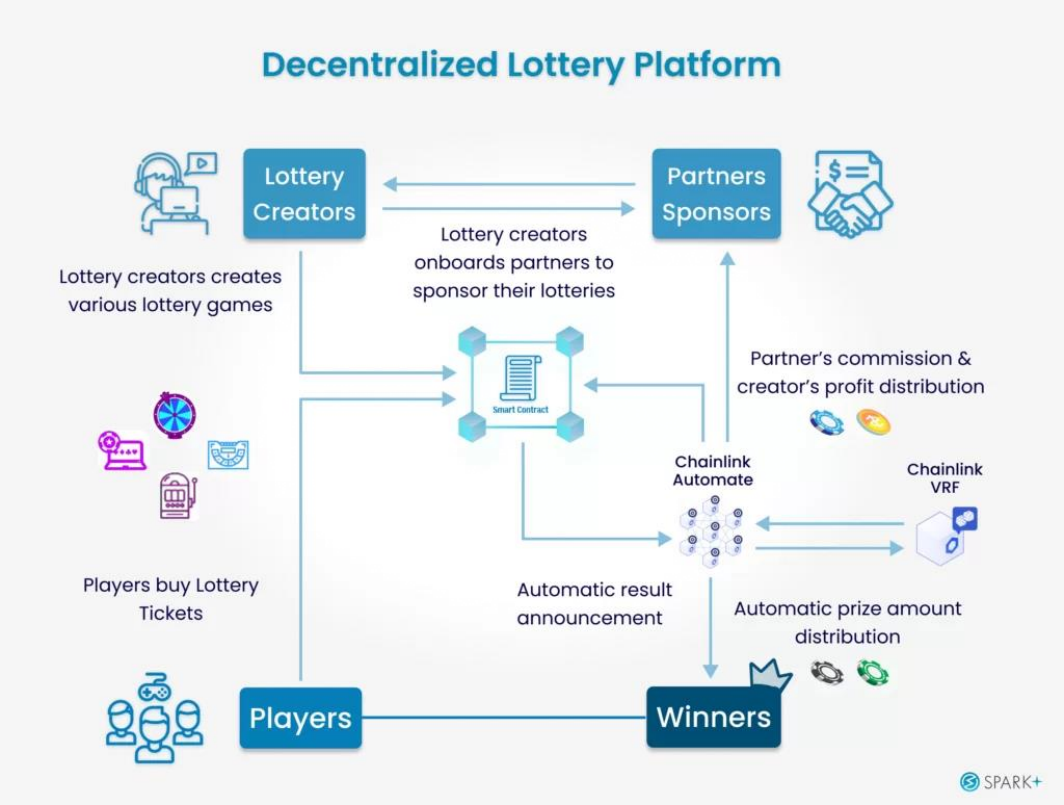

Fig. 4.1: Flow Chart of decentralized lottery system

Fig4.1 decentralized lottery platform leverages smart contracts to ensure transparency, automation, and fairness. Lottery creators develop games and onboard partners/sponsors, while players buy tickets to participate. The system uses Chainlink VRF for random winner selection and Chainlink Automate for automatic result announcements and prize distribution. Partners receive commissions, and winners get rewards securely. This blockchain-powered model eliminates intermediaries, ensuring a fair, efficient, and trustless lottery ecosystem.

Audited Code – Conduct third-party audits to identify vulnerabilities and enhance contract security.

Reentrancy Protection – Use the **Checks-Effects-Interactions** pattern to prevent reentrancy attacks.

Overflow/Underflow Prevention – Utilize **SafeMath** or Solidity's built-in safeguards to avoid errors.

Access Control – Implement **role-based access control (RBAC)** to restrict administrative functions.

Time-Locking Mechanisms – Delay high-risk transactions to prevent flash loan exploits.

Zero-Knowledge Proofs (ZKPs) – Use **ZK-SNARKs** or **ZK-STARKs** to verify transactions privately.

Stealth Addresses – Generate one-time addresses for lottery ticket purchases to ensure anonymity.

.

4.5Benefits

Transparency – All transactions are recorded on the blockchain, ensuring a tamper-proof lottery system.

Fairness – Provably fair **random number generators (RNGs)** eliminate fraud or manipulation.

Security – Smart contracts automate processes, reducing human errors and hacking risks.

Decentralization – No single entity controls the lottery, making it more democratic and trustless.

Lower Costs – Eliminates intermediaries, reducing operational costs and increasing prize payouts.

Instant Payouts – Winnings are automatically distributed via smart contracts without delays.

5 IMPLEMENTATION

Requirements and Tools

Before starting the implementation, make sure you have the following tools and libraries:

Ethereum: The blockchain platform for deploying the smart contract.

Solidity: The programming language for writing smart contracts on Ethereum.

MetaMask: A browser extension wallet for managing Ethereum accounts and interacting with the blockchain.

Truffle or **Hardhat**: Development frameworks for compiling, testing, and deploying smart contracts.

Ganache: A personal Ethereum blockchain for testing and development purposes.

Infura or Alchemy: Services that provide access to the Ethereum mainnet/testnet for deployment.

Web3.js or **Ethers.js**: JavaScript libraries for interacting with the smart contract in the front-end.

5.1: Smart Contract Design

The smart contract should handle the following tasks:

1. **Ticket Sales**: Allow users to purchase lottery tickets.
2. **Random Number Generation**: Ensure fair random winner selection.
3. **Prize Distribution**: Automatically distribute the prize to the winner.
4. **Lottery End Conditions**: Define when the lottery starts and ends.

A basic design flow:

1. Users buy tickets by sending Ethereum to the contract.
2. After a set number of tickets are purchased or a time limit is reached, the contract draws a winner.
3. The winner receives the prize directly into their Ethereum wallet.

5.2: Writing the Smart Contract in Solidity

Here's an example of a simple lottery smart contract:

solidity

Copy

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract Lottery {
    address public manager; // Manager of the lottery
    address[] public players; // Array to store participants
    uint256 public ticketPrice = 0.1 ether; // Price per lottery ticket
    uint256 public maxPlayers = 100; // Max number of players
    uint256 public lotteryEndTime;

    constructor() {
        manager = msg.sender; // The person who deploys the contract is the manager
       lotteryEndTime = block.timestamp + 1 days; // Lottery lasts for 1 day from deployment
    }

    function enter() public payable {
        require(msg.value == ticketPrice, "Incorrect ticket price");
        require(block.timestamp < lotteryEndTime, "Lottery has ended");
        require(players.length < maxPlayers, "Max players reached");

        players.push(msg.sender); // Add player to the lottery pool
    }

    function pickWinner() public restricted {
        require(block.timestamp >= lotteryEndTime, "Lottery is still ongoing");
        require(players.length > 0, "No players in the lottery");

        uint256 randomIndex = random() % players.length; // Pick a random winner
        address winner = players[randomIndex];

        payable(winner).transfer(address(this).balance); // Transfer the prize money to the winner
```

```
        // Reset the lottery for the next round
        players = new address Clear the players array
        lotteryEndTime = block.timestamp + 1 days; // Set the end time for
the next round
    }

    function random() private view returns (uint256) {
        return         uint256(keccak256(abi.encodePacked(block.difficulty,
block.timestamp, players)));
    }

    modifier restricted() {
        require(msg.sender == manager, "You are not the manager");
        _;
    }
}
```

Explanation of the Code:

1. **Manager**: The address that deploys the contract (typically the owner or administrator) can call restricted functions, like picking the winner.
2. **Ticket Sales**: The `enter()` function allows participants to buy tickets. It accepts an amount of **Ether** equal to `ticketPrice`, checks if the time and player conditions are met, and then adds the player to the lottery pool.
3. **Lottery End**: The lottery ends after 24 hours, or when the maximum number of players is reached.
4. **Winner Selection**: The `pickWinner()` function is used to randomly select a winner and transfer the prize amount (the total balance of the contract) to the winner.
5. **Random Number Generation**: The `random()` function generates a pseudo-random number based on `block.difficulty`, `block.timestamp`, and the participants' addresses. Note that this is not completely secure and may be vulnerable to manipulation. A more secure method like **Chainlink VRF** should be used in production environments.
6. **Resetting the Lottery**: After each lottery, the contract resets the players and sets the lottery end time for the next round.

5.3: Testing the Smart Contract

Truffle or Hardhat: Use frameworks like **Truffle** or **Hardhat** to write unit tests for the smart contract. This ensures that all functions (e.g., ticket purchasing, winner selection, prize distribution) work correctly and securely.

5.5: Interacting with the Smart Contract

Once the contract is deployed, you can interact with it using a **web interface** or **CLI**. Use **Web3.js** or **Ethers.js** to interact with the deployed contract.

For example, using **Ethers.js** to buy a lottery ticket and pick a winner:

```
javascript
Copy
const { ethers } = require("ethers");

const provider = new ethers.JsonRpcProvider("YOUR_INFURA_URL");
const signer = provider.getSigner();
const lotteryAddress = "YOUR_DEPLOYED_CONTRACT_ADDRESS";
const lotteryABI = [ /* Your Contract's ABI */ ];

const lotteryContract = new ethers.Contract(lotteryAddress, lotteryABI, signer);

// Buy a ticket
await lotteryContract.enter({ value: ethers.utils.parseEther("0.1") });

// Pick the winner
await lotteryContract.pickWinner();
```

5.6: Frontend Interface

To make the lottery more user-friendly, you can develop a **frontend interface** using **HTML/CSS** and **JavaScript**. You can use **React** or **Vue.js** for more interactive and dynamic interfaces. The frontend can allow users to:

View current lottery details (e.g., ticket price, number of participants).

Enter the lottery by sending ETH.

View the winner and the prize distribution in real-time.

6 ADVANTAGES

A **lottery smart contract using blockchain technology** offers numerous advantages that traditional, centralized lottery systems cannot provide. These advantages enhance fairness, transparency, security, and efficiency, among other factors. Below are the key benefits:

6.1. Transparency and Trust

One of the most significant advantages of using blockchain technology for a lottery is the **transparency** it provides. Since all transactions on a blockchain are publicly visible and immutable, participants can independently verify the entire lottery process, from ticket purchases to the selection of winners. This transparency builds trust, ensuring that there is no manipulation or fraud involved.

Key points:

Public ledger: Every action is recorded, visible to all participants.

Tamper-proof: Once data is written to the blockchain, it cannot be altered or erased.

6.2. Security

Blockchain's inherent **security features** are another major advantage. The decentralized nature of blockchain ensures that there is no central authority or server that can be attacked, hacked, or compromised. All data is stored across multiple nodes in a distributed manner, which makes it difficult for malicious actors to manipulate or alter the lottery results.

Key points:

Encryption: Blockchain transactions are encrypted, offering a high level of data security.

Decentralization: Reduces the risk of hacking or fraud, as no single point of failure exists.

6.3. Fairness in Winner Selection

Blockchain-based lotteries often rely on **verifiable randomness** for selecting winners. This ensures that the process is not biased and that no external party can influence the outcome. Techniques like **Verifiable Random Functions (VRFs)** are used to generate secure random numbers, which can be independently verified by anyone, ensuring that winners are chosen in a completely fair manner.

Key points:

Provably fair: Participants can independently verify that the randomness used to select winner is genuine and not manipulated.

No human intervention: The automated nature of smart contracts ensures that the process is free from human error or manipulation.

6.4. Lower Operational Costs

Traditional lottery systems often require significant infrastructure and administrative costs, such as ticket printing, distribution, and verification**. With a blockchain-based lottery,** middlemen **and** physical infrastructure **are eliminated, reducing overhead costs. Smart contracts handle ticket purchases, draw events, and prize payouts automatically, which results in red**

uced operational expenses.

Key points:

- **No intermediaries**: No need for third-party management or verification.
- **Automation**: Smart contracts automate processes, reducing the need for human intervention and minimizing errors.

6.5. Global Accessibility

Blockchain technology provides a **decentralized and borderless environment**, allowing participants from anywhere in the world to join the lottery, provided they have internet access and a cryptocurrency wallet. This opens up the lottery system to a global audience and eliminates geographical restrictions, making it more inclusive than traditional lotteries that are often limited to specific regions or countries.

Key points:

- **Cross-border participation**: Anyone with internet access can participate, regardless of location.
- **Inclusive**: Provides access to people who may not otherwise have the opportunity to engage in traditional lotteries.

7.CHALLENGES

While the implementation of a **lottery smart contract using blockchain technology** offers numerous advantages, it also presents several challenges that need to be addressed for the system to operate effectively. These challenges include:

7.1. Randomness Generation

One of the key challenges in blockchain-based lotteries is ensuring **true randomness** for selecting winners. Blockchain environments are deterministic, meaning the outcome of any operation can be predicted by anyone who has access to the blockchain data. Most blockchain networks do not have an inherent source of randomness, which can lead to biased results if not carefully handled. Solutions like **pseudo-random number generators (PRNGs)** or **Verifiable Random Functions (VRFs)** are commonly used, but they still face challenges in guaranteeing absolute fairness

7.2. Scalability

As the number of participants in the lottery grows, the blockchain network may face **scalability** issues. High transaction volumes could lead to network congestion, causing delays and higher transaction fees. This could make the system less efficient, especially if the lottery becomes popular. Finding a blockchain solution that scales effectively while maintaining low fees is crucial for large-scale adoption.

7.3. Security and Smart Contract Bugs

Smart contracts are immutable once deployed, meaning any bugs or vulnerabilities in the code cannot be easily fixed. If a smart contract contains a bug, it could be exploited by malicious actors, leading to financial losses or unfair outcomes in the lottery. Ensuring robust **security audits** and thorough testing of the smart contract code is vital to minimize the risks associated with vulnerabilities.

7.4. Regulatory and Legal Challenges

Blockchain-based lotteries might face **regulatory and legal** challenges, especially in jurisdictions where gambling or lottery systems are heavily regulated.

8 CONCLUSION

In conclusion, the development of a **lottery smart contract using blockchain technology** represents a transformative shift in how traditional lottery systems operate. By leveraging the inherent transparency, security, and decentralization of blockchain, this system addresses key challenges in conventional lotteries, such as fraud, manipulation, and lack of transparency. Through **smart contracts**, the lottery process is automated, ensuring fairness and efficiency by eliminating intermediaries and reducing operational costs.

Blockchain technology also enables **global accessibility**, allowing participants from anywhere in the world to join, as long as they have internet access and a digital wallet. This promotes inclusivity and expands opportunities for participation beyond geographic boundaries. The integration of verifiable random number generation ensures that the winner is selected in a fair and unbiased manner, further building trust in the system

.

While there are challenges, such as ensuring true randomness and addressing scalability concerns, the benefits far outweigh these hurdles. The blockchain lottery system offers increased **security**, **transparency**, and **accountability**, creating a level playing field for all participants. It also encourages **economic growth** by fostering innovation in the gaming and finance sectors and potentially reducing inequalities by making lottery opportunities more accessible.

In summary, a blockchain-based lottery system is a more efficient, fair, and secure alternative to traditional lotteries. As blockchain technology continues to evolve, it is likely to open new avenues for digital innovation, creating more equitable and transparent systems across industries.

9 SDG's ADDRESSED

A decentralized marketplace powered by blockchain technology contributes significantly to multiple **United Nations Sustainable Development Goals (SDGs)** by fostering transparency, security, and efficiency while promoting fair trade and economic inclusion. Below are the key SDGs addressed by your decentralized marketplace:

SDG 9: Industry, Innovation, and Infrastructure

- **Description**: Build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation.
- **Relevance**: The implementation of a lottery smart contract on blockchain is a technological innovation that disrupts traditional lottery systems, offering a more transparent, secure, and decentralized model. This aligns with the goal of fostering innovation in digital infrastructure and decentralizing systems.

How the project contributes:

- Introduces a decentralized, transparent, and secure lottery system.
- Promotes blockchain technology as an infrastructure for new industries, especially in gaming and finance.

SDG 16: Peace, Justice, and Strong Institutions

- **Description**: Promote peace, justice, and inclusive societies, and build effective, accountable, and inclusive institutions at all levels.
- **Relevance**: By leveraging blockchain's transparency and immutability, the lottery smart contract ensures fairness and accountability in the lottery process, reducing the potential for corruption or fraud.

How the project contributes:

- Ensures fairness and transparency, eliminating corruption in lottery operations.

- Builds trust with users due to the verifiability of the system, reinforcing strong institutions.

SDG 12: Responsible Consumption and Production

- **Description**: Ensure sustainable consumption and production patterns.
- **Relevance**: A blockchain-based lottery can be designed to reduce waste and improve efficiency. By automating lottery processes via smart contracts, administrative costs and human intervention are minimized, making the system more efficient and eco-friendly.

How the project contributes:

- Reduces the need for paper-based processes or physical ticket sales.
- Streamlines the production and consumption of lottery services, contributing to more efficient and sustainable operations.

4. SDG 10: Reduced Inequality

- **Description**: Reduce inequality within and among countries.
- **Relevance**: The decentralized nature of the blockchain ensures that lottery opportunities are available to anyone with internet access, eliminating barriers often associated with centralized, traditional lottery systems (like regional access limitations).

How the project contributes:

- Provides equal access to all participants across the globe.
- The decentralized structure ensures that no centralized authority has control over the process, promoting fairness and equal opportunities.

10. REFERENCES

- **Buterin, V. (2013).** *Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform.* Ethereum. Available at: https://ethereum.org/whitepaper **(pp. 23-24)**
- .**Wood, G. (2014).** *Ethereum: A Secure Decentralized Generalized Transaction Ledger.* Ethereum Foundation. Available at: https://ethereum.github.io/yellowpaper/paper.pdf **(pp. 5-6)**

- **Vera, J., & Antonopoulos, A. M. (2016).** *Mastering Ethereum: Building Smart Contracts and DApps.* O'Reilly Media. **(pp. 253-255)**
- **Nakamoto, S. (2008).** *Bitcoin: A Peer-to-Peer Electronic Cash System.* Bitcoin.org. Available at: https://bitcoin.org/bitcoin.pdf **(pp. 1-9)**
- **Narula, R., & Yadav, M. (2020).** *Blockchain Technology and its Applications. Journal of Computer Applications, 43(2),* 21-27. **(pp. 25-26)**.
- **Chainlink. (2021).** *Chainlink VRF: Verifiable Random Function.* Chainlink Documentation. Available at: https://chain.link/vrf **(pp. 12-14)**
- **Hertig, A. (2020).** *The Power of Smart Contracts: Blockchain's Revolutionary Application in Various Industries. Journal of Technology and Innovation, 16(1),* 45-60. **(pp. 50-52)**

11 APPENDIX A

https://drive.google.com/drive/folders/1fjZbX-_v_KgGPzJ6-HZpQ591xC3olq_0