iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41695

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Secured Lottery System Using Smart Contract and Blockchain Technology

Arihant Duggar[1], Divyanshu Gupta[2], Royal[3], Mohan C.G[4]
[1, 2, 3, 4]*Vellore Institute of Technology, Vellore, Tamil Nadu*

Abstract: ***To create a lottery based smart contract on ethereum blockchain for increasing transparency and reduce frauds in the lottery industry. Once the contract has been deployed by the administrator, there will be a minimum contribution amount for players to register in the game and a price pool will be maintained by the smart contract. The winning process will be structured in a way such that only the administrator's wallet will be authorized to initiate the process to randomly pick an address and the smart contract will by definition transfer the prize to the winner. The contract once deployed on blockchain cannot be changed by the administrator to maintain transparency and fairness.***
Keywords: Smart contract, lottery system, application of ethereum, blockchain technology.

I. INTRODUCTION

Blockchain is developing as one of the most important technologies that affect our day-to-day life. It is structured in a way that allows you to create records in a safe and transparent way. Each block in the blockchain contains the data transaction, timestamp and hash of the previous block. It is not feasible to forge the data which enables the data to be reliable in the blockchain. The turning characteristic of the blockchain is the significant use of encryption used as a link element between blocks. Accommodation of a lottery system in a blockchain can result in increased transparency. There is an urgent need to replace traditional systems with fully computerized systems that ensure fairness.

Transparency and fair distribution of funds are all the most common issues that most people doubt, distrust, or complain about. When playing the lottery, the winning percentage is determined purely by chance without skill. Lottery players are not classic gamblers. Lottery players rely entirely on opportunities, hoping that they have the potential to thrive and win life-changing awards, and a small amount of money to buy the dream of becoming an instant millionaire. Each participant purchases a ticket in anticipation of the realization of their dreams. Under the current system, there are intermediaries and distributors who sell lottery tickets to people in each region.

The rest of the process, such as auditing and declaring results, is also manually performed by the intermediary under government obedience. In this system, people are concerned about unpredictability and consistency, as well as random number fairness, testability, and tamper resistance. And based on these facts, we have equipped the blockchain with a lottery buying and selling process. Evaluate payments, tickets and payments in the distribution environment using blockchain technology. The blockchain network allows all players to participate on an equal footing. There is no central concept of power, but power is distributed to all involved. The lottery process involves certain steps such as registration, purchase, completion, verification, random selection of winners, announcement of winners, and payment. The security of payment, ticketing and payment in the sales environment is guaranteed by the system using the blockchain.

II. INNOVATIVE TECHNOLOGY

Blockchain technology brings reliability and security without the need to rely on the intermediate to operate during a transaction[1]. A blockchain platform, Ethereum[5], supports the execution of intelligent agreements. Ethereum can provide the ability to build and provide distributed applications on an open platform basis. It is one of the important concepts that are a small computer program called "life" of the blockchain.

This is part of the code that runs on the blockchain. While blockchain technology was limited to the field of financial transactions, the advent of smart contracts has expanded the fame of blockchain technology to many other fields such as the lottery. Blockchain smart contracts improve blockchain scalability by allowing developers to program their own applications without the need for blockchain migration.

III. BLOCKCHAIN

Blockchain is a distributed ledger technology. It is a timeless digital ledger of economic transactions. You can record virtually anything of value on the blockchain, not just financial transactions. It is a structure consisting of blocks containing transaction records, consisting of multiple heterogeneous records in multiple databases called "chains" of networks connected by competitors' nodes. This storage is commonly referred to as the "digital ledger." This allows you to distribute digital information, but you cannot post it. This means that each piece of data can only have one owner, and linking blocks to the chain makes the information stored on the blockchain reliable. Blockchain is a distributed database that provides a secure, transparent and decentralized way to execute, record, and validate all types of transactions. Blockchain eliminates the need for centralized management by decentralizing all transactions, and validation is done by the distributed ledger blockchain database itself. The blockchain consists of three core parts: blocks, chains, and networks. The block records a list of transactions over a period of time in your ledger. A chain is a hash that connects one block to another. Create a hash using the data from the previous block. This is a data typogram that clamps blocks in order and time. A network is a collection of nodes. Each node contains a complete record of all transactions previously recorded on the associated blockchain. Running a node is expensive and time consuming.

IV. ETHEREUM

Ethereum was launched in 2015. Ethereum is a prominent open source, public, distributed, and blockchain-based computing platform that emphasizes smart contract capabilities.

Ethereum is currently ideal for building decentralized applications. Ethereum is an open source blockchain-based pulpit that provides developers with the ability to build and set up decentralized applications. Ethereum is a platform that enables people to conveniently create decentralized applications using blockchain technology.

At the Ethereum blockchain, Prospectors strive to acquire Ethereum, a type of crypto token that strengthens the network. Ethereum is a pulpit for the global exchange of information that cannot be used or changed. Ethereum, also known as ETH, is a decentralized digital currency.

V. SMART CONTRACT

In simple words, intelligent contracts are a small computer program that runs in the blockchain "life" or blockchain. Issuing an intelligent contract is not only applicable to a lawyer, but also a blockchain in other areas such as lottery. Two human agreements in the form of computer code. Intelligent agreements are performed in the blockchain and thus stored in the published database and can not be changed. Transactions that occur in intelligent agreements are treated by blockchains. In other words, they can be sent automatically without a third party.

Ethereum is a distributed computing platform that generates cryptocurrency tokens called Ethereum. Smart contracts are automatically executed based on the code programmed by the programmer on the Ethereum blockchain. Ethereum virtual machines are used to execute these contracts that consist of all the devices running on the Ethereum node.

The "Distributed Platform" part means that anyone can set up and run an Ethereum node by paying the operator of the Ethereum node, which is the cryptocurrency token associated with Ethereum. Therefore, computing power will be available to and paid for by those who are running Ether.

VI. CRYPTOGRAPHIC RANDOM FUNCTION

The random function is used in the contract to generate and pick a random winner and hence transfer the total amount of winning ethers in his registered account.

In order to generate a winner, we are first generating a random number based on a cryptographic hash function and then picking an index from the players array as a winner. The index to be selected as a winner is calculated by performing modulus of length of players array operation on the generated random number.

Example: uint index = random() % players.length

A. Method of Generating Random Number

Random=(keccak256(abi.encodePacked(block.difficulty, block.timestamp, players)));

The random number is generated by encrypting the block difficulty , block timestamp and players address array using Keccak256 hash algorithm.

VII. ETHEREUM CONTRACT

A. *Recording the Manager's Address by Deploying the Contract*

Initially the address of the manager will be recorded to identify the deployer of the contract, to achieve this we can make use of the globally available msg object in the constructor function. This msg object has various properties attached to it. For example, we have a value, a sender, gas, and a data property on it. The msg.sender inside a constructor function is the address of the account which initially deployed the contract.

B. *Players Purchasing the Lottery to Participate*

A public payable type function must be created. If the player contributes more than the minimum Ethers specified by calling the function, the player's address must be stored using msg.sender and pushed into an array of address payable type. This players array will contain addresses of all the eligible participants for the prize money.

When the player calls the function in order to buy the lottery tickets, the amount he/she pays can be recorded using msg.value. The msg.value must be greater than the minimum specified value set by the administrator. For example, if we want the players to contribute a minimum of 0.1 ethers then we can use, require(msg.value > .1 ether).

C. *Pick Winner with the help of Random Number Generator*

Construct a random number by converting the hash of current block difficulty, timestamp and wallet addresses of all the players in the game generated by Keccak256 algorithm into an integer reduced to the range of the number of players. The random number is the index position of the winner in the player list. The lottery amount is then transferred to the winner's ethereum wallet.

Pseudocode:

```
contract lottery
{
   declare address manager;
   declare payable[] public players;

   constructor() {
      set  manager to msg.sender;

   }

   function enter() public payable {
      if msg.value > .01 ether
         push payable(msg.sender) to players;

   }

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

   function pickWinner() public restricted {
      uint index = random() % players.length;
      players[index].transfer(address(this).balance);
      players = new address payable[](0);
   }

   function pickWinner() public restricted {
      set uint index to random() % players.length;
      transfer balance to  players[index];
```

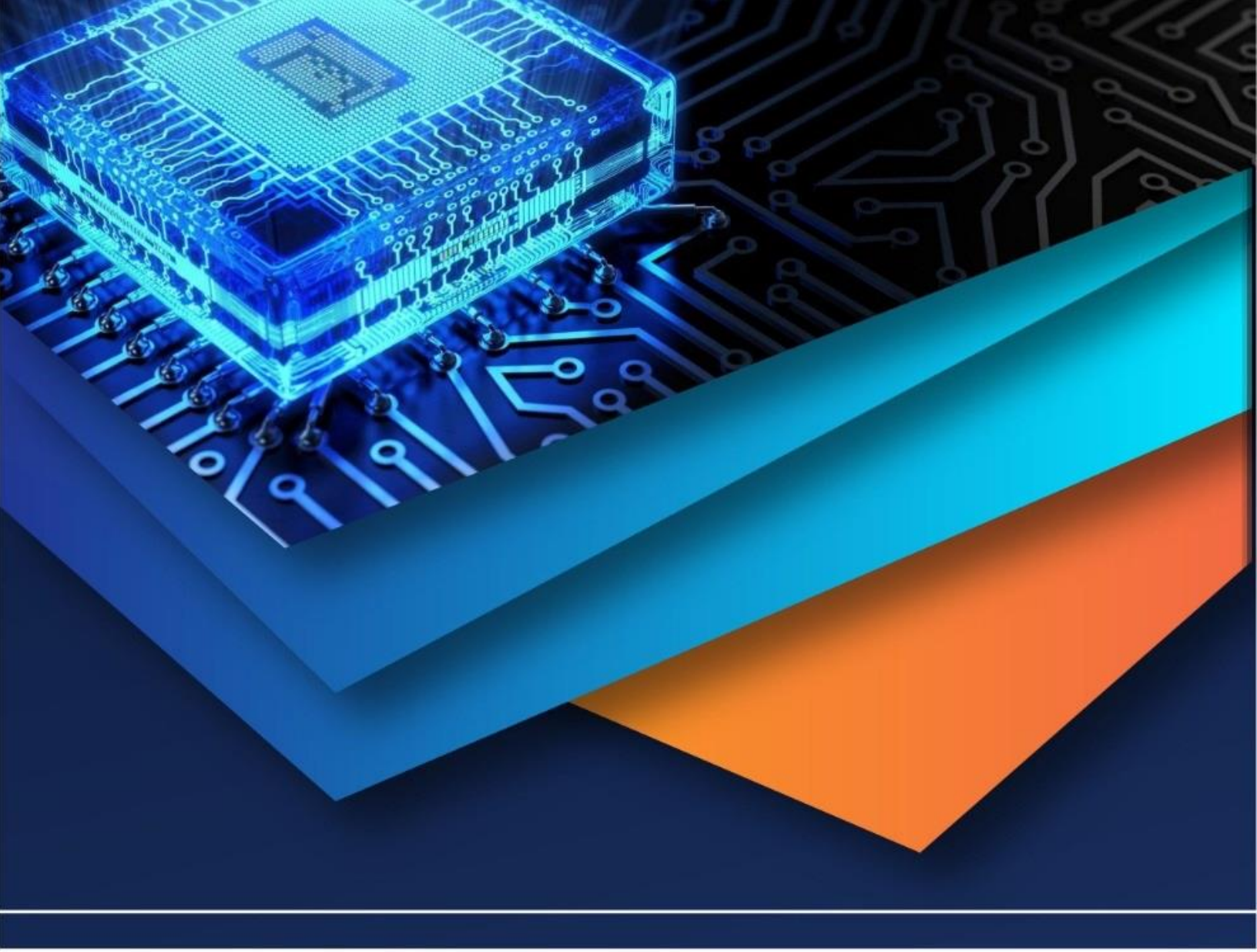
```
        initialize players to a new address payable[](0);
    }

    function modifier restricted() {
        if msg.sender == manager;
            _;
    }

    function getPlayers() public view returns (address payable[] memory) {
        return players;
    }

}
```

VIII. CONCLUSION

This paper introduces a new methodology using the Blockchain and Ethereum network in the process of selling and purchasing lottery tickets . This system will replace the original lottery operations in every aspect such as the removal of third-parties in the buying process, ensuring the efficiency in prize declaration and the claiming of prizes. The winning number can be generated through the proposed random number generator. Each record regarding the purchase will be stored on blockchain and also the prize details and thus provides a verifiable and transparent system for the participants. In general, this system can curtail almost every preeminent problem of the traditional lottery and it ensures fairness to the consumer as well.

REFERENCES

[1] Mathews Emmanuel, Nimmy Chacko and T Anagha, A Blockchain based SmartContract Digitized Lottery Scheme
[2] K. Chatterjee, A. K. Goharshady and A. Pourdamghani, Probabilistic Smart Contracts: Secure Randomness on the Blockchain.
[3] Da-Yin Liao,Xuehong Wang, Design of a Blockchain-Based Lottery System for Smart Cities Applications.
[4] Daniel Macrinici, Cristian Cartofeanu, Shang Gao, Smart contract applications within blockchain technology.
[5] Liao, D.-Y.; Wang, X., Applications of Blockchain Technology to Logistics Management in Integrated Casinos and Entertainment.
[6] Rouhani, Sara & Deters, Ralph, Security, Performance, and Applications of Smart Contracts.
[7] Luon-Chang Lin1,2 and Tzu-Chun Liao, A Survey of Blockchain Security Issues and Challenges.
[8] Xin Sun ,Piotr Kulicki,ORCID and Mirek Sopek, Lottery and Auction on Quantum Blockchain.
[9] Zhifeng Jia , Rui Chen , Jie Li, DeLottery: A Novel Decentralized Lottery System Based on Blockchain Technology.
[10] Pichada Saichua, Sawitree Khunthi, Thawatchai Chomsiri, Design of Blockchain Lottery for Thai Government.
[11] Kexin HuEmail ,Zhenfeng Zhang, Fast Lottery-Based Micropayments for Decentralized Currencies.
[12] Harry Halpin,Marta Piekarska “Introduction to Security and Privacy on the Blockchain.
[13] Ashish Sharma, Dinesh Bhuriya, Blockchain security and Technology.
[14] Andhir Kumar Rakesh Tripathi, Secure Healthcare Framework Using Blockchain and Public Key Cryptography.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY