A Project Report on

**DECENTRALISED LOTTERY SYSTEM USING BLOCKCHAIN**

***Submitted in partial fulfillment of the requirement for the award of the degree of***

Bachelor of Technology in Computer Science and

Engineering



**Under The Supervision of**

**Mr. Anupam Lakhanpal**

**Assistant Prof.**

**Department of Computer Science and Engineering**

Submitted By

**19SCSE1010529 – SHIVANK MANGAL**

**19SCSE1010511 – PRADEEP PANDEY**

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

### GALGOTIAS UNIVERSITY, GREATER NOIDA INDIA

#### May, 2022

**SCHOOL OF COMPUTING SCIENCE AND**

**ENGINEERING**

**GALGOTIAS UNIVERSITY, GREATER NOIDA**

## CANDIDATE’S DECLARATION

I/We hereby certify that the work which is being presented in the project, entitled

“DECENTRALISED LOTTERY SYSTEM USING BLOCKCHAIN” in partial fulfillment of the requirements for the award of the BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING submitted in the School of Computing Science and Engineering of Galgotias University, Greater Noida, is an original work carried out during the period of JANUARY-2022 to MAY-2022, under the supervision of Mr. ANUPAM LAKHANPAL, Assistant Professor, Department of Computer Science and Engineering of School of Computing Science and Engineering , Galgotias University, Greater Noida The matter presented in the project has not been submitted by me/us for the award of any other degree of this or any other places.

19SCSE1010529 – SHIVANK MANGAL

19SCSE1010511 – PRADEEP PANDEY

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Supervisor

(Mr. Anupam lakhanpal, Assistant Professor)

# 

# **CERTIFICATE**

The Final Thesis/Project/ Dissertation Viva-Voce examination of

19SCSE1010529 -SHIVANK MANGAL, 19SCSE1010511 - PRADEEP PANDEY has been held on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and his/her work is recommended for the award of BACHELOR OF TECHNOLOGY IN

COMPUTER SCIENCE AND ENGINEERING.

Signature of Examiner(s) Signature of Supervisor(s)

#### Signature of Project Coordinator Signature of Dean

Date:

Place:

# **ABSTRACT**

In this paper, we design DeLottery, a decentralized lottery and gambling system based on block chain technology and smart contracts. Lottery is a classical form of entertainment and charity for centuries. Facing the bottleneck of the combination between lottery and information technology, we use smart contracts and blockchain in decentralized, intelligent, and secure systems for lottery industries. Moreover, we are inspired by the algorithm of RANDAO, an outstanding way of random number generation in blockchain scenario.

The components and the functions of the novel system are described in details.

Plenty of illegal lottery companies are gradually banned by governments during the past 10 years, and online lottery system has become a sensitive issue. We implement Decentralised Lottery in a blockchain network and show functioning procedure and security of the proposed lottery system.

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Table Name** | **Page No.** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| 8 |  |  |
| 9 |  |  |

**TABLE OF CONTENTS**

Title Page i

Certificate ii

Declaration iii

Acknowledgment iv

Abstract v

List of Figures vi

List of Tables viii

1. **INTRODUCTION 1**
   1. Objective
   2. Problem Definition
   3. Existing System
2. **LITERATURE SURVEY**
3. **METHODOLOGY** 
   1. System Design
   2. Modules
   3. Technologies Used
   4. Diagrammatic Representation
      1. Data Flow Diagram

UML Diagram

* 1. Implementation of Proposed solution
  2. System Requirements

1. **RESULTS AND DISCUSSIONS**
2. **CONCLUSION AND FUTURE WORK**

**REFERENCES**

**appendex**

# CHAPTER 1

**INTRODUCTION**

Lottery is a financial activity where people pay money for their bets, in most cases, certain sequences of numbers, and then they have chances to win prizes [1]. The current prevailing lottery system functions as follows: (1) A lottery company starts a lottery; (2) People make bets and pay money; (3) The lottery company generate winner numbers randomly; (4) Winners collect their prizes. Suppose that there are certain number participants taken part in a lottery event, hosted by a lottery company or organization. For a typical event, the parameters are listed in Table 1.The fairness of lotteries depends mostly on the third parties These companies as the centers of these activities are trusted by participants. They set the rules and regulations which are supposed to be equal to every individual. The lottery events are usually hosted by lottery companies or governments, and the whole procedure of a lottery event often takes an entire day. The clumsiness of a host company or organization is preventing the traditional lottery system from high efficiency. When it comes to large traditional lottery events, it often takes the third party around 24 hours to collect the lottery tickets, making the traditional lottery process quite time-consuming and inconvenient for individuals to host lottery events. People have been aware of the inconvenience, and stepped forward with the proposal of web-based lottery system. Back in 1999, David Leason and Scott L. Sullivan developed a type of online lottery system with centralized feature. The system design was among one of the greatest contributions to the traditional lottery system, and it fulfilled people’s need for instantly hosting lottery events in a relatively convenient way. In the last decade, a large number of lottery companies emerge, and influenced the traditional lottery business. However, the covenant- lite online lottery systems often fail to guarantee their users with the fundamental need for security, both in the sense of information security that their personal information is not leaked, and property security that their legal rewards can be guaranteed.

## Objective

## Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the “chain,” in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital ledger

## **1.2.Problem Definition**

The lottery is a type of gambling which involves the drawing of specific numbers to win the large prizes. Many people consider it as a gaming product, but it is a high volume industry which can also be called as a commodity.

## Existing System

## The traditional lottery procedure takes a relatively long period, and it is quite inconvenient for individuals to hold a lottery event in a traditional way.

## If the third party fails to be totally fair while producing the winners, benefits of the players are hurt.

## It is possible that the third party pay the winners a less amount of money or even nothing so that the third party itself can have some more interests. Proposed System .

One of the lottery directors said, “Lotteries are different from any other gaming product. Lottery players risk a small amount of money against very long odds to win a large prize, with the net proceeds going to the public good.”

The lottery industry keeps a 29% share of the entire global gambling revenue.

Increased from $187.1 billion in 2004 to $284.3 billion in 2014, the global lottery represented an annual growth rate of 4.3% over ten years.

But with the growth of the digital economy, the industry faces challenges like the lack of transparency and fairness.

The world demands more transparency and fairness with advanced technologies like blockchain.

The distributed nature of blockchain promises innovation in the lottery industry.

# CHAPTER 2

# LITERATURE SURVEY

##### Smart contracts are regarded as one of the most promising and appealing notions in blockchain technology.

##### Their self-enforcing and event-driven features make some online activities possible without a trusted third party. Nevertheless, problems such as miscellaneous attacks, privacy leakage,

##### and low processing rates prevent them from being widely applied. Various schemes and tools have been proposed to facilitate the construction and execution of secure smart contracts. However,

##### a comprehensive survey for these proposals is absent, hindering new researchers and developers from a quick start. This paper surveys the literature and online resources on smart contract construction and execution over the period 2008–2020. We divide the studies into three categories:

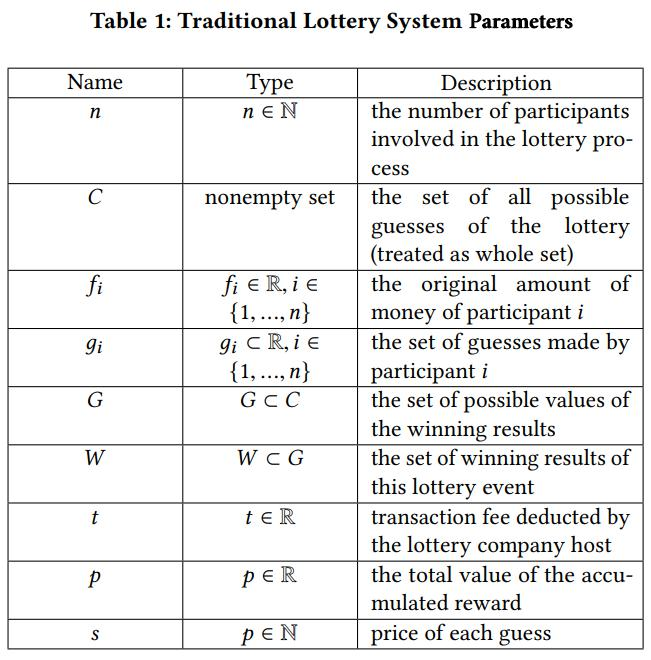
##### design paradigms that give examples and patterns on contract construction,

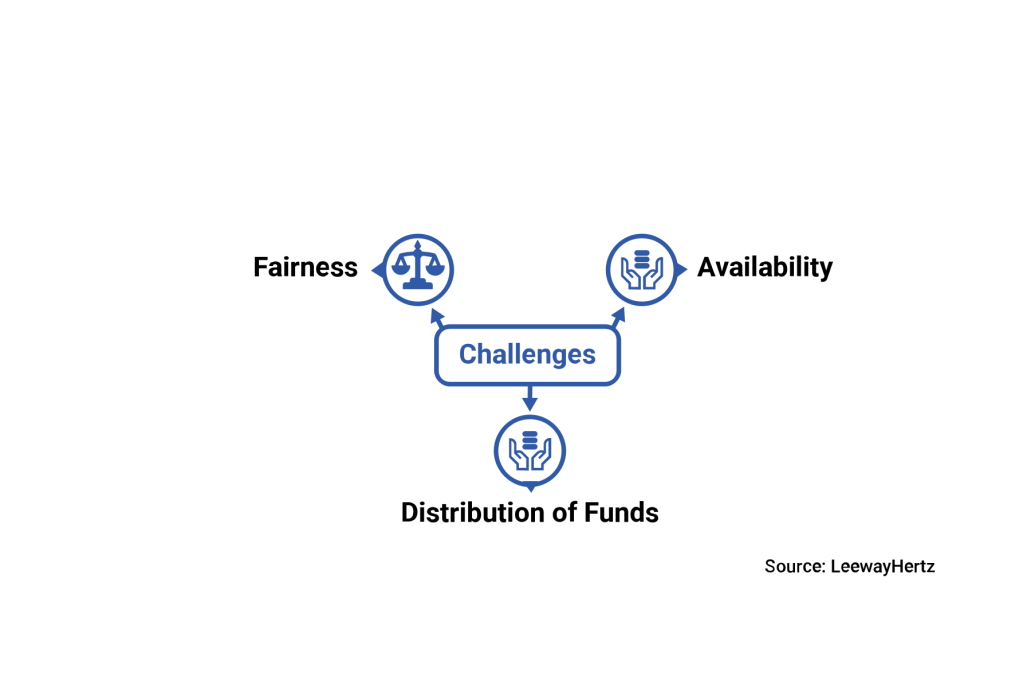
##### design tools that facilitate the development of secure smart contracts, and

##### extensions and alternatives that improve the privacy or efficiency of the system.

##### We start by grouping the relevant construction schemes into the first two categories. We then review the execution mechanisms in the last category and further divide the state-of-the-art solutions into three classes: private contracts with extra tools, off-chain channels, and extensions on core functionalities. Finally, we summarize several challenges and identify future research directions toward developing secure, privacy-preserving, and efficient smart contracts.

##### Table 1: Literature Review





****Fairness-****

It is essential to ensure the integrity of the games to avoid the risks of manipulation or frauds. Lottery players doubt the fairness of lotteries and ask the following questions:

Are the deal and ticket real or not?

Is the random number generation (RNG) method secure and random?

Are the prizes paid on time? Is the jackpot winner real?

Is the money accumulated in one pool and used for social causes?

Since the traditional lotteries fail to answer the above questions, lotteries lack fairness in the system.

**Here are some of the real cases of manipulation in the lottery industry:**

**The 1980 Pennsylvania Lottery Scandal (The Triple Six Fix)**

The scandal of Pennsylvania was a plot to rig the Daily Number, a three-digit number. Except the balls numbered 4 and 6, all the balls in three machines were weighted. Therefore, it was sure the drawn number could be a combination of 4s and 6s.

The planned scheme got successful as 666, one of the eight combinations of 6s and 4s, was drawn on April 24, 1980. The fix led to a significant change for the lotteries.

The illicit winnings were never paid out while the chief conspirators were imprisoned.

**Hot Lotto Fraud Scandal (IOWA Lottery Case)**

Eddie Raymond Tipton, former information security director of the Americal Multi-State Lottery Association, affirmed to rigging RNG that he and two others used in various cases of state lotteries frauds.

He installed a software code which enabled him to modify RNG and guess winning numbers on specific dates of the year. Because of the altered RNG, he won a $14.3 million jackpot in 2010.

As a result, Tipton was convicted and sentenced to ten years imprisonment in 2015.

Therefore, it is essential to bring fairness to the lottery systems.

**Availability**

Due to the smaller size of the domestic market, users from different countries cannot get involved in the biggest lotteries in the world. They are restricted to participate in smaller local lotteries.

Though new online solutions enable players to purchase worldwide or US lottery tickets, the service charges and risks of fraud and mismanagement are higher.

As of now, the state and law regulations control the way lotteries are carried out in different corners of the world. On an average, not more than 50% of funds gathered from ticket sales are issued to the prize pool.

Also, the lottery participants have no control over how much money should be collected from ticket sales, and lottery winnings are taxed in some countries.

**Distribution of Funds**

Lotteries are served as funding for charity and other social projects. But in many cases where countries have high levels of corruption, players can question the fair distribution of funds.

Since there is no way to get information about the distribution of funds, it could be the biggest challenge for the players to build trust in the specific lottery association.

Because the blockchain is a distributed ledger technology with a secure write-forward authentication system, it can add data without the risk of a single point of failure. Every node involved in the blockchain network has a copy of the ledger.

Users can update the information into the ledger without the involvement of a third party. It gives individuals more power and flexibility.

Therefore, the blockchain can be well implemented in the lottery or gambling industry.

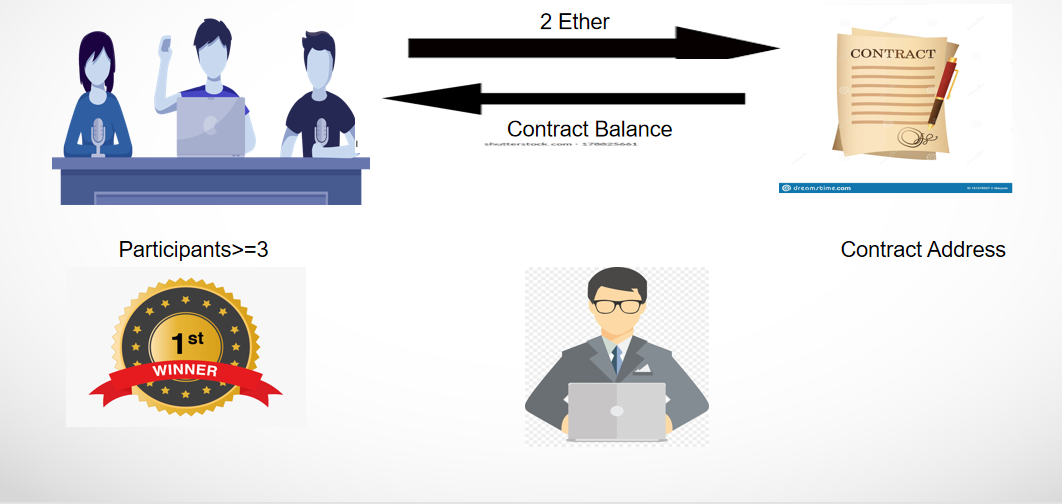
# CHAPTER 3

# METHODOLOGY

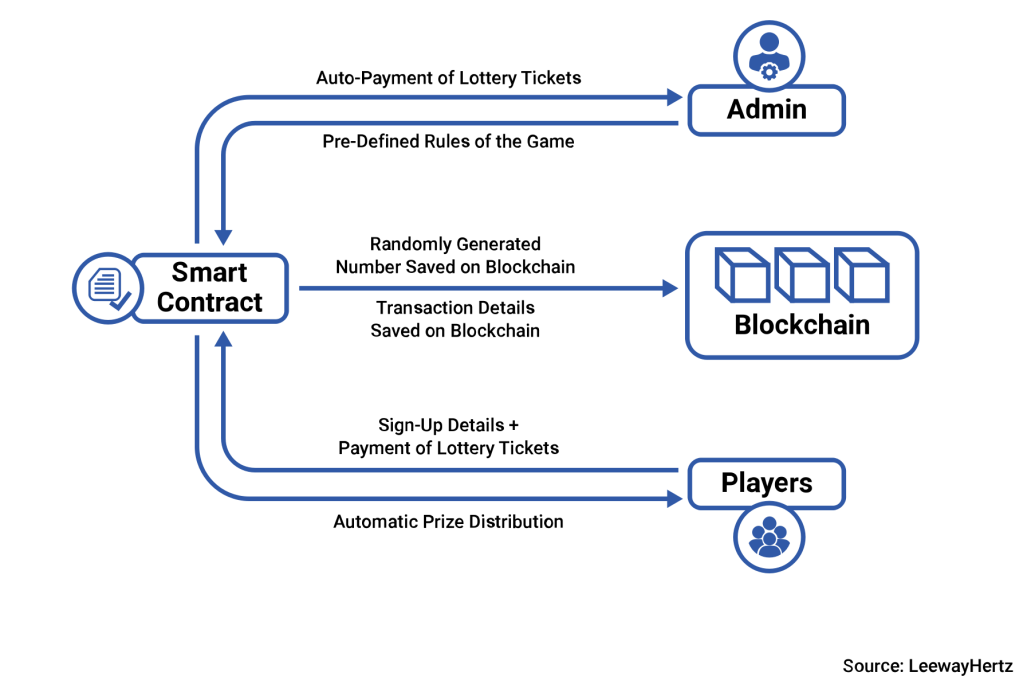
We have developed a smart contract for our model.

## System Design

Describes the data flow in a diagrammatic representation.



**Figure 3.1** System model



****Technology components involved in the blockchain lottery process:****

* Public Blockchain
* Android/iOS App or Web Platform for Players
* Web Platform for Admins to deploy smart contracts

### ****Step 1: Players sign up to the lottery platform****

Lottery players need to sign up to the platform to participate in the lottery and become its member.

They sign up to the **blockchain lottery** system with the following information

* Name
* Wallet Address
* Email Id
* Phone Number

After the successful sign-up, players can get alerts and notifications related to ticket openings on a regular basis.

### ****Step 2: Admin announces the ticket openings and deploys the smart contracts****

Admin announces the ticket openings on the platform and the notification is sent to the users. They also deploy smart contracts, which contain pre-defined rules for the lottery game to bring fairness and transparency to the ecosystem.

Smart contracts ensure what information should be shared with which stakeholder in the system, providing privacy and disclosure of data.

Since the players can buy the tickets with cryptocurrencies, their identities remain anonymous. The transactions stored on a public blockchain allows traceability and makes it easier to resolve disputes/scandals related to lotteries.

### ****Step3 : A Random number is generated and recorded on the blockchain****

Since the random number generator is based on the blockchain, the algorithm relies on recent random blockchain transactions. It pulls a specified amount and order of numbers to generate each winning number sequence.

Because nobody is aware of the next transaction in the blockchain, the lottery platform adds an extra layer of randomness to the selection process.

Once the random number is generated and matched to the player’s ticket number, they are awarded and money is automatically sent to their respective wallets.

The funds to be distributed to players are defined in the smart contracts.

Therefore, the decided commissions and funds are paid out to every player on the platform.

Moreover, the smart contract code is available publically on the platform; players can check the rules defined in the contracts to confirm if the funds are distributed in a fair way or not.

### ****Step 4: Players can trace back the history of records of transactions****

Since the transactions are recorded on the blockchain, players can trace back the history to know who had won the jackpot and if the commissions and wins are paid out as defined in the smart contracts.

**Technologies used:**

> SOLIDITY

>REMIX IDE

>METAMASK WALLET

>SMART CONTRACT

>BLOCKCHAIN

1. **SOLIDITY-**

Solidity is an object-oriented programming language created specifically by the Ethereum Network team for constructing and designing smart contracts on Blockchain platforms. It's used to create smart contracts that implement business logic and generate a chain of transaction records in the blockchain system.

Solidity also shares similar characteristics to the programming languages C++ and Python. As a high-level language, Solidity does away with the need to type code in ones and zeros. It makes it much easier for humans to write programs in ways they find easier to understand, using a combination of letters and numbers.

1. **. BLOCKCHAIN-**

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant’s ledger. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT).

Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash.

1. **. SMART CONTRACT-**

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

Smart contracts work by following simple “if/when…then…” statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

**(4). METAMASK-**

* MetaMask is a cryptocurrency wallet that enables users to store Ether and other ERC-20 tokens.
* The wallet can also be used to interact with decentralized applications, or dapps.

MetaMask is one of the leading crypto **[wallets](https://decrypt.co/?post_type=post&p=5702" \t "https://decrypt.co/resources/blank)**, and aims to be the gateway to the world of Web 3, decentralized finance (DeFi) and [NFTs](https://decrypt.co/resources/non-fungible-tokens-nfts-explained-guide-learn-blockchain" \t "https://decrypt.co/resources/_blank).

[MetaMask](https://metamask.io/" \t "https://decrypt.co/resources/_blank) is a browser plugin that serves as an **[Ethereum](https://decrypt.co/?post_type=post&p=5726" \t "https://decrypt.co/resources/blank)** wallet, and is installed like any regular plugin. Once it's installed, it allows users to store Ether and other [ERC-20](https://decrypt.co/resources/erc20" \t "https://decrypt.co/resources/_blank) tokens, enabling them to make transactions to any Ethereum address.

By connecting to Ethereum-based dapps, users can spend their coins in games, stake tokens in gambling applications and trade them on decentralized exchanges ([DEXs](https://decrypt.co/resources/what-is-decentralized-exchange-dex" \t "https://decrypt.co/resources/_blank)).

It also provides users with an entry point into the emerging world of decentralized finance, or **[DeFi](https://decrypt.co/?post_type=post&p=25908" \t "https://decrypt.co/resources/blank)**, providing a way to access DeFi apps such as [Compound](https://decrypt.co/resources/compound-defi-ethereum-explained-guide-how-to" \t "https://decrypt.co/resources/_blank) and [PoolTogether](https://decrypt.co/resources/what-is-pooltogether-the-no-loss-crypto-lottery-explained" \t "https://decrypt.co/resources/_blank).

# Diagrammatic Representation

#### Data flow diagram

A data flow diagram (DFD) maps out the flow of information for any process or system. It uses defined symbols like rectangles, circles and arrows, plus short text labels, to show data inputs, outputs, storage points and the routes between each destination. Data flowcharts can range from simple, even hand-drawn process overviews, to in-depth, multi-level DFDs that dig progressively deeper into how the data is handled. They can be used to analyze an existing system or model a new one. Like all the best diagrams and charts, a DFD can often visually “say” things that would be hard to explain in words, and they work for both technical and nontechnical audiences, from developer to CEO. That’s why DFDs remain so popular after all these years. While they work well for data flow software and systems, they are less applicable nowadays to visualizing interactive, real-time or database-oriented software or systems.

#### 3.4.2 DFD digram

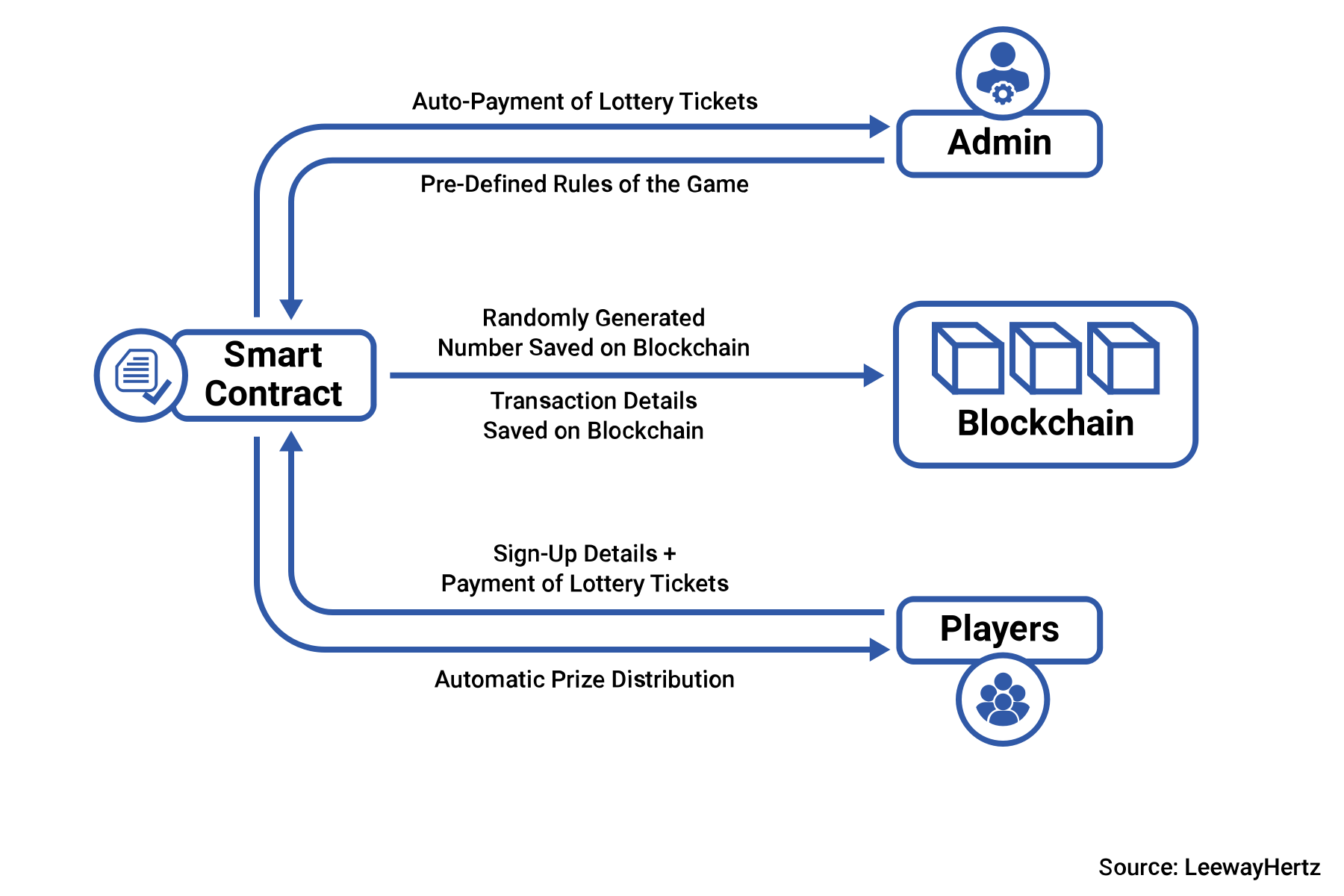


Fig- 3.4.3

****Technology components involved in the blockchain lottery process:****

* Public Blockchain
* Android/iOS App or Web Platform for Players
* Web Platform for Admins to deploy smart contracts.
  + 1. **UML Diagrams**

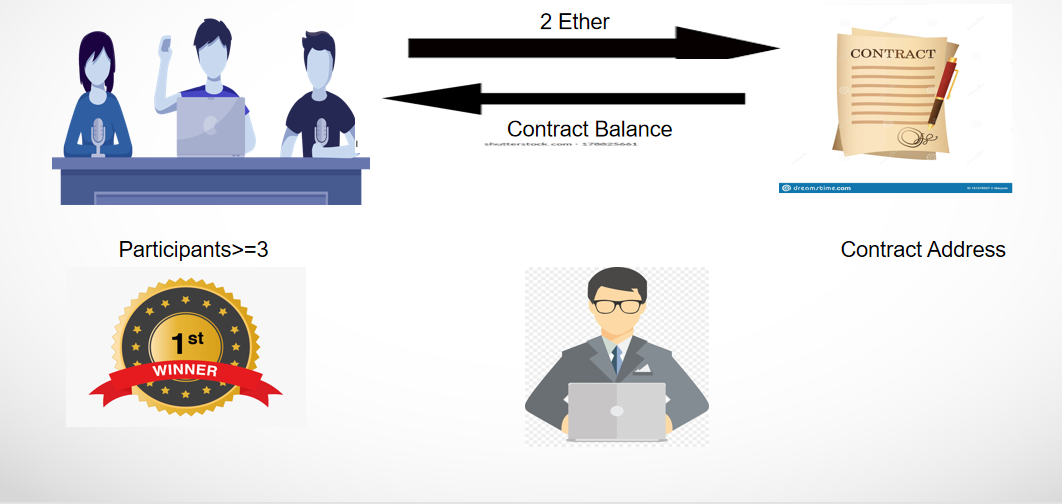
UML is the international standard notation for object-oriented analysis and design. The object management group defines it. The heart of object-oriented problem solving is the construction of a model. The model abstracts the essential details of the underlying problem from its usually complicated real world. The scope UML is a language for specifying artifacts, visualizing artifacts, constructing artifacts and documenting artifacts. UML provides the following diagrams to represent the software process:

* Class Diagram
* Use Case diagram
* Sequence diagram

#### Class Diagram

class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects.

The class diagram is the main building block of object-oriented modeling. It is used for general conceptual modeling of the structure of the application, and for detailed modeling translating the models into programming code. Class diagrams can also be used for data modeling. The classes in a class diagram represent both the main elements, interactions in the application, and the classes to be programmed.



**Figure 4.2.3** Class diagram

#### Use Case Diagram

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well. The use cases are represented by either circles or ellipse.

## Algorithms and Techniques-

**Source code-**

//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{

    address payable[] public players;

    address public manager;

    constructor(){

        manager = msg.sender;

    }

    receive () payable external{

        require(msg.value == 0.1 ether);

        players.push(payable(msg.sender));

    }

    function getBalance() public view returns(uint){

        require(msg.sender == manager);

        return address(this).balance;

    }

    function random() internal view returns(uint){

       return uint(keccak256(abi.encodePacked(block.difficulty, block.timestamp, players.length)));

    }

    function pickWinner() public{

        require(msg.sender == manager);

        require (players.length >= 3);

        uint r = random();

        address payable winner;

        uint index = r % players.length;

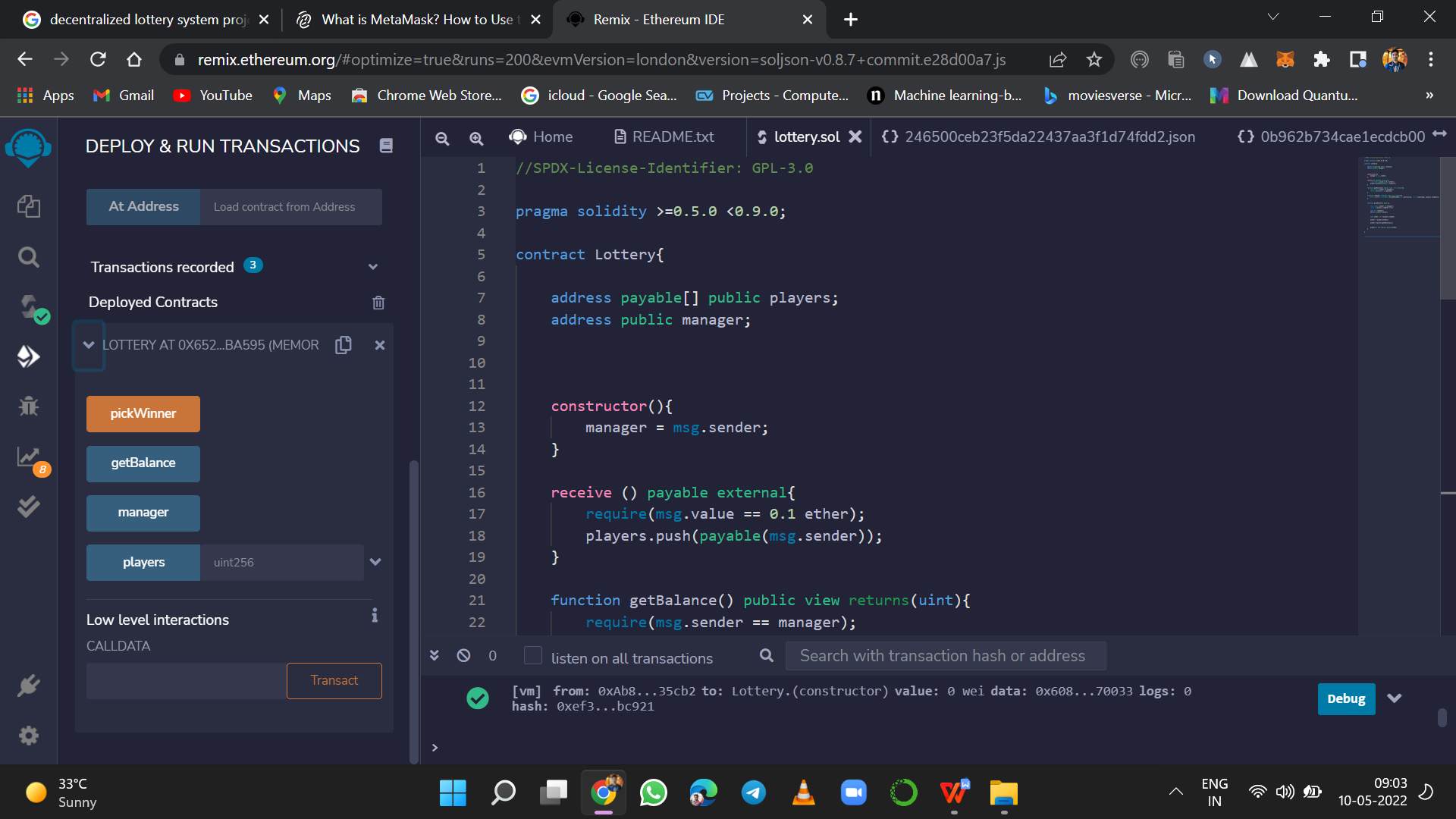
        winner = players[index];

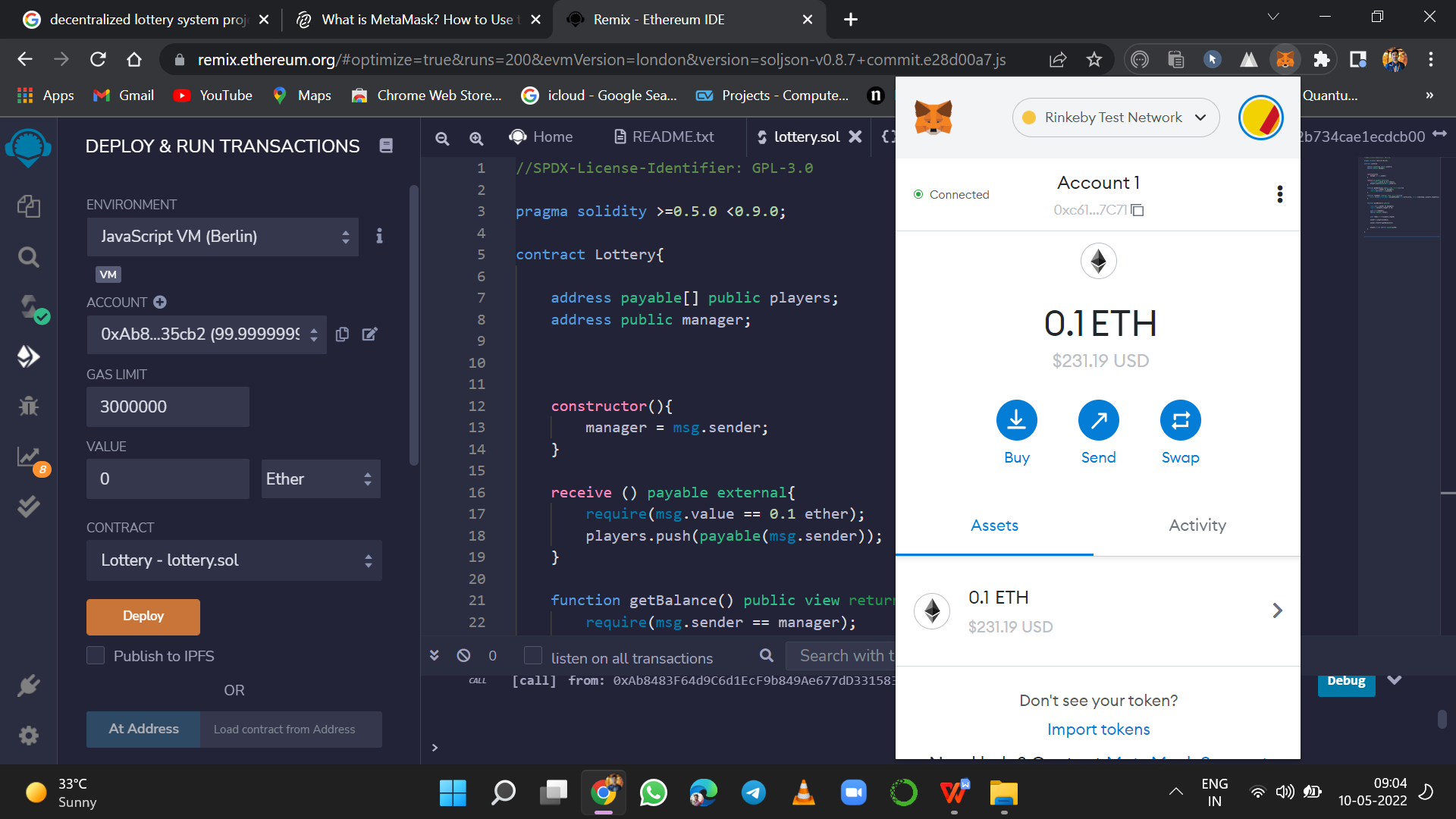
        winner.transfer(getBalance());

        players = new address payable[](0);

    }

}





* 1. **System Requirements**
     1. Windows 11, 7, 8, 10, .
     2. MacOS, iOS
     3. Language Used: solidity, JavaScript
     4. IDE : remix ide,
     5. **Browsers**
        1. Chrome
        2. Internet Explorer
        3. Firefox
        4. Safari
        5. Edge
     6. **Hardware Requirements**

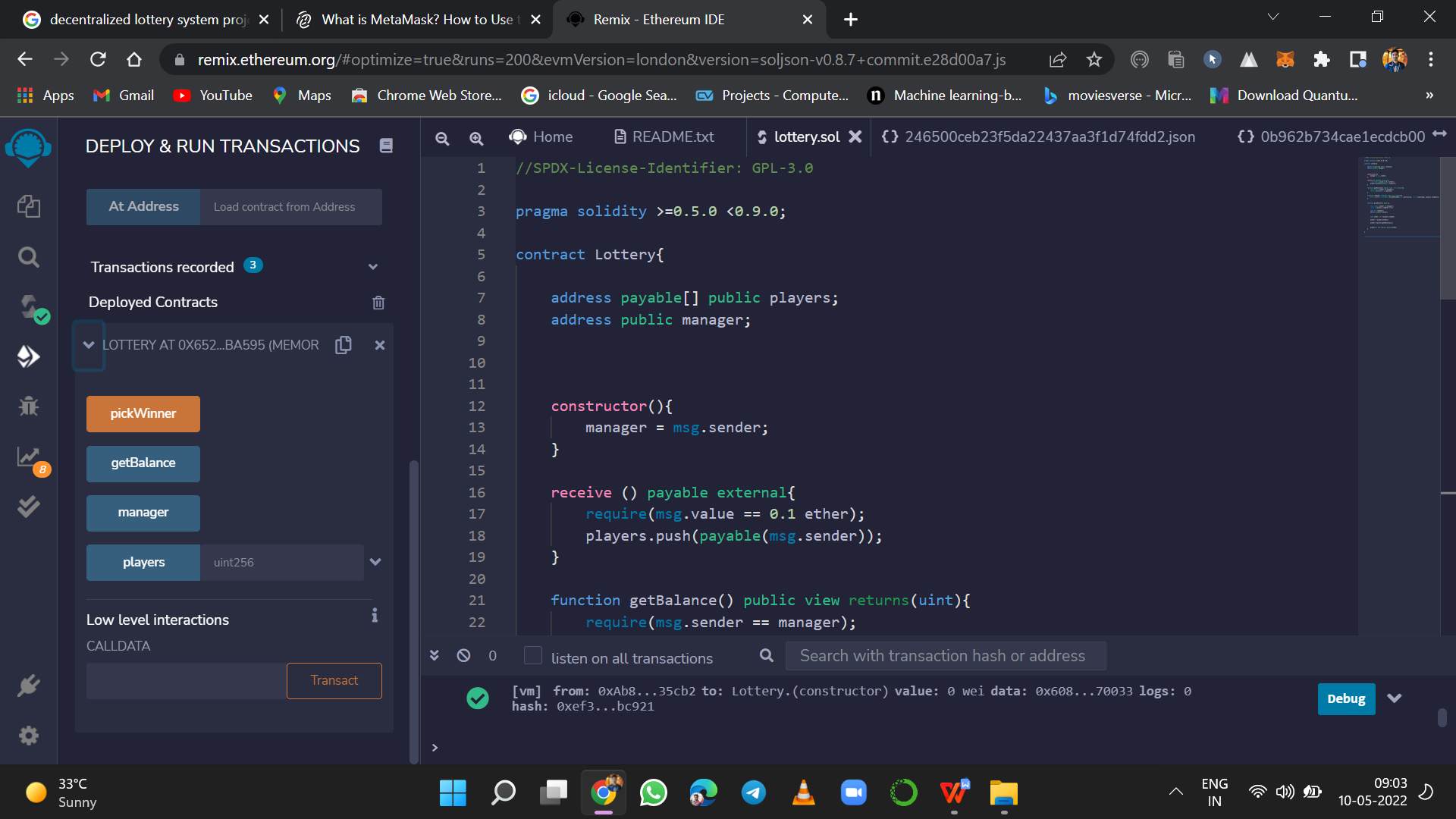
1. System : Intel core i5
2. Hard Disk : 20 GB
3. Monitor : Virtual Machine: Standard D4s v3
4. Ram : 16 GB

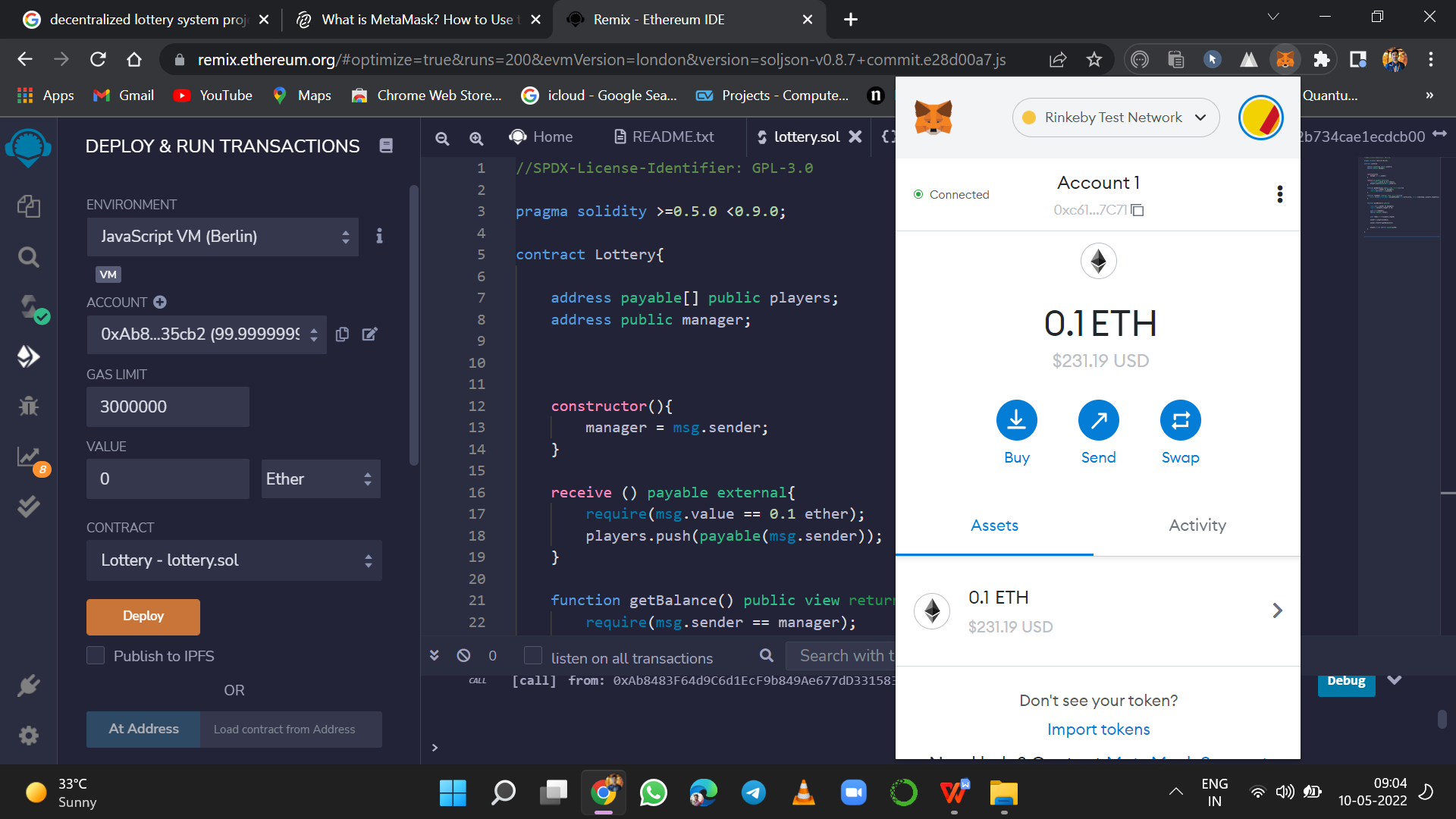
# CHAPTER 4

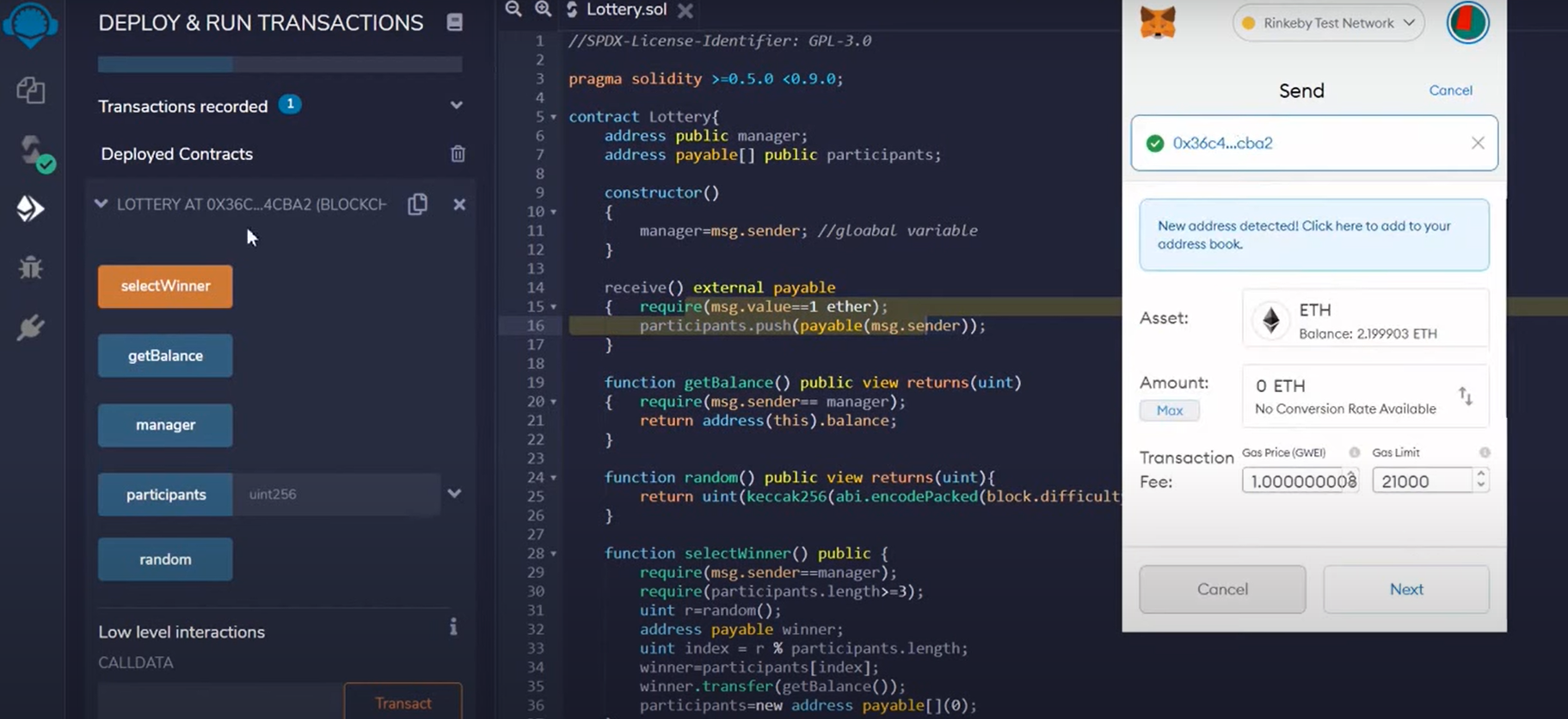
# RESULTS AND DISCUSSIONS

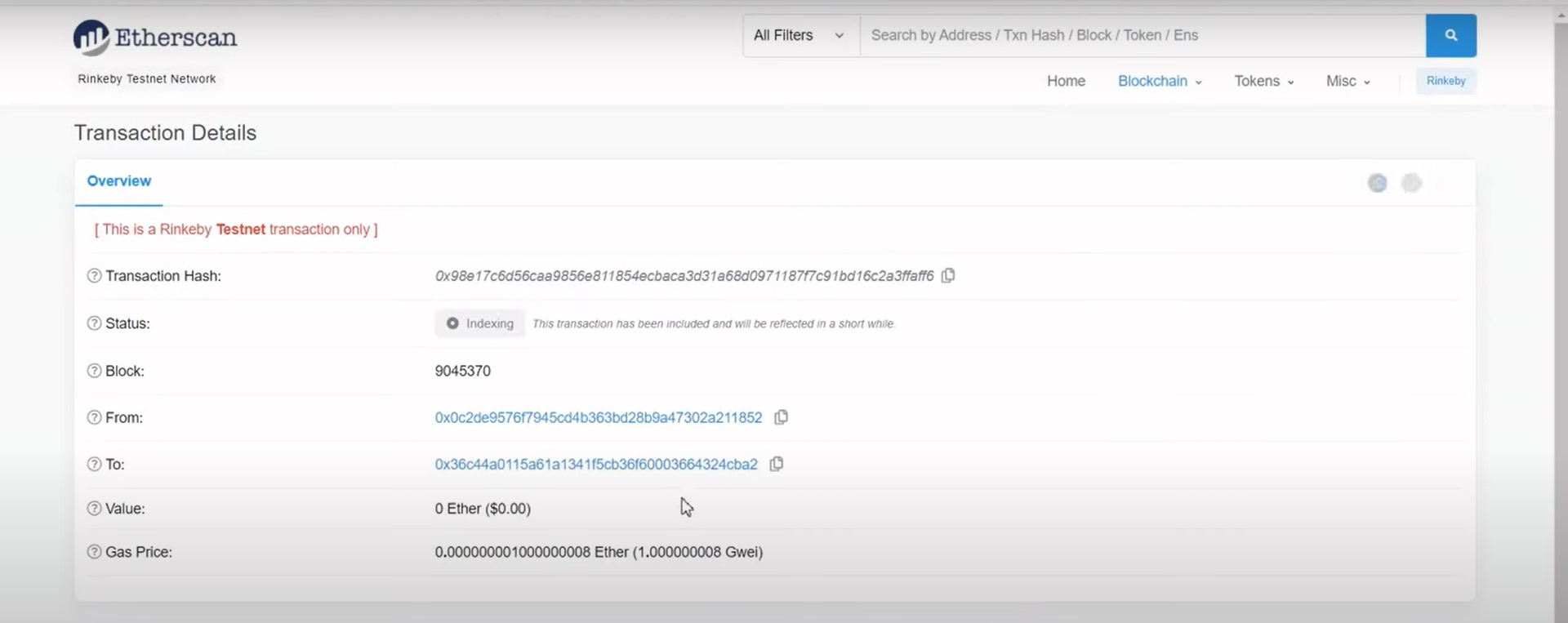
Deploying contracts btw 4 parties

1. Pick winner
2. Getbalalnce
3. Manager
4. player









# CHAPTER 5

# CONCLUSION AND FUTURE WORK

## Conclusions

We described a framework for the distribution of tokens to final users new to blockchain tools.

The system is completely decentralized, non custodial, and provides a seamless user experience.

The process was tested on the Ethereum main net during an event held at Politecnico di Milano in January 2020.

Observations show that costs are comparable to those of a centralized solution, even though they could be further reduced by using new experimental technologies such as rollups.

Further possible work includes the evaluation of distributed key generation for the generation of the redeeming keys.

## Future Work

As known, two issues in using public blockchains are fees volatility and scalability. In the remainder,

we consider different strategies for reducing fees and improving the throughput and latency of our system.

# REFERENCES

[1] Thomas Barker and Marjie Britz. 2000. Jokers wild: Legalized

gambling in the twenty-first century. Greenwood Publishing

Group.

[2] Guido Bertoni, Joan Daemen, MichaÃńl Peeters, and Gilles

Van Assche. 2013. Keccak. (2013).

[3] S. Bragagnolo, H. Rocha, M. Denker, and S. Ducasse. 2018.

SmartInspect: solidity smart contract inspector. In 2018

International Workshop on Blockchain Oriented Software

Engineering (IWBOSE). 9–18.

https://doi.org/10.1109/IWBOSE.2018. 8327566

[4] Y. Chen, S. Chen, and I. Lin. 2018. Blockchain based smart

contract for bidding system. In 2018 IEEE International

Conference on Applied System Invention (ICASI). 208–211.

https://doi.org/10.1109/ICASI.2018.8394569

[5] K. Christidis and M. Devetsikiotis. 2016. Blockchains and

Smart Contracts for the Internet of Things. IEEE Access 4

(2016), 2292–2303. https://doi.org/10.1109/

ACCESS.2016.2566339

[6] Itai Dinur, Orr Dunkelman, and Adi Shamir. 2012. New

Attacks on Keccak-224 and Keccak-256. In International

Conference on Fast Software Encryption.

[7] Da-Yin Liao and Xuehong Wang. 2017. Design of a

Blockchain-Based Lottery System for Smart Cities

Applications. In Collaboration and Internet Computing (CIC),

2017 IEEE 3rd International Conference on. IEEE, 275–282.

[8] M. Mettler. 2016. Blockchain technology in healthcare: The

revolution starts here. In 2016 IEEE 18th International

Conference on e-Health Networking, Applications and Services

(Healthcom). 1–3.

https://doi.org/10.1109/HealthCom.2016.7749510

[9] B. K. Mohanta, S. S. Panda, and D. Jena. 2018. An Overview

of Smart Contract and Use Cases in Blockchain Technology. In

2018 9th International Conference on Computing,

Communication and Networking Technologies (ICCCNT). 1–4.

https://doi.org/10.1109/ICCCNT.2018.8494045

[10] RANDAO. 2018. RANDAO White Book on Provable Fair

Random Number Generation.

[11] S. Rouhani and R. Deters. 2017. Performance analysis of

ethereum transactions in private blockchain. In 2017 8th IEEE

International Conference on Software Engineering and Service

Science (ICSESS). 70–74. https://doi.org/10.1109/ICSESS.

2017.8342866

[12] George Sher. 1980. What makes a lottery fair? Noûs (1980),

203–216.

[13] Emin GÃĳn Sirer. 2017. How Not To Run A Blockchain

Lottery. http:// hackingdistributed.com/2017/12/24/how-not-to-

run-a-blockchain-lottery/

[14] F. Tschorsch and B. Scheuermann. 2016. Bitcoin and Beyond:

A Technical Survey on Decentralized Digital Currencies. IEEE

Communications Surveys Tutorials 18, 3 (thirdquarter 2016),

2084–2123. https://doi.org/10.1109/COMST.2016.2535718

[15] Henk C. A. van Tilborg and Sushil Jajodia (Eds.). 2011.

Proof of Work. Springer US, Boston, MA, 984–984.

https://doi.org/10.1007/978-1-4419-5906-5\_1060

[16] E. Yavuz, A. K. KoÃğ, U. C. ÃĞabuk, and G. DalkÄślÄśÃğ.

2018. Towards secure evoting using ethereum blockchain. In

2018 6th International Symposium on Digital Forensic and

Security (ISDFS). 1–7.

https://doi.org/10.1109/ISDFS.2018.8355340

[17] Choi S Park S Smolander K Yli-Huumo J, Ko D (Ed.). 2016. .

PLoS ,ONE, Boston.

## Loading the model

**Lottery.sol**

//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{

address payable[] public players;

address public manager;

constructor(){

manager = msg.sender;

}

receive () payable external{

require(msg.value == 0.1 ether);

players.push(payable(msg.sender));

}

function getBalance() public view returns(uint){

require(msg.sender == manager);

return address(this).balance;

}

function random() internal view returns(uint){

return uint(keccak256(abi.encodePacked(block.difficulty, block.timestamp, players.length)));

}

function pickWinner() public{

require(msg.sender == manager);

require (players.length >= 3);

uint r = random();

address payable winner;

uint index = r % players.length;

winner = players[index];

winner.transfer(getBalance());

players = new address payable[](0);

}

}