CCMP 603 - Introduction to Smart Contracts

Lottery Smart Contract Project

Instructor:

Mayra Samaniego MSc. Ph.D. (c)

Members:

Hai-Nam, Nguyen - 000520322

Xuan Hieu, Nguyen - 000518043

Cong Chi Tai, Nguyen - 000516006

Table of content

I. Purpose of the Lottery Smart Contract

Our Lottery Smart Contract aims to build a decentralized and open lottery system that runs on the Ethereum blockchain. With the help of a fair and trustworthy platform provided by this smart contract, players will be able to enter a lottery and have a chance to win a prize through a process of random selection. The Lottery Smart Contract has the following primary goals and purposes:

Transparency: The smart contract ensures complete transparency in the lottery process. All participants can verify the fairness of the lottery by examining the contract's code and the blockchain's immutable ledger. Every action and transaction in the game is documented on the blockchain based on blockchain technology. The prize fund, the winner, and the prize distribution can all be seen by players.

Security: By using blockchain technology and smart contracts, our lottery system minimizes the risk of fraud and manipulation, creating a secure environment for participants. Blockchain technology uses cryptography to protect the system from hackers.

Decentralization: The lottery operates on a decentralized network, eliminating the need for centralized authority. The player can trust that the result is accurate and not manipulated.

Fairness: The random selection process used in the lottery makes sure that each player has an equal chance of winning. It eliminates bias and prevents outside influences from having an impact on the selecting process.

Automated Payouts: When the lottery concludes, the smart contract automatically distributes the prize to the winning participant based on predefined rules, removing the need for manual intervention. This guarantees that the winner gets paid out fast and effectively.

Cost Efficiency: By eliminating paperwork and the dependence on third parties for verifying transactions, operating on blockchain reduces administration costs associated with running a traditional lottery system. Participants only pay gas fees when interacting with the contract.

Accessibility: This lottery system is open to everyone with an Ethereum wallet, reaching a global audience.

Immutable Results: Once the lottery has concluded, the results are recorded on the blockchain and cannot be changed, ensuring the integrity of the outcome.

In conclusion, the Lottery Smart Contract uses blockchain technology to change conventional lottery systems by bringing transparency, security, and fairness. It offers a fresh, decentralized method for running lotteries while making sure that players can believe in the procedure automated payouts and outcomes with immutable results.

II. Parties that participate in Lottery Smart Contract

In design of the Lottery Smart Contract, we agreed that there would be three main parties involved:

Participants/Players: These are individuals who want to participate in the lottery. They interact with the smart contract to buy lottery tickets by sending transactions to the contract. Each player has a chance to win the lottery based on the rules and random selection mechanism defined in the contract.

Contract Creator/Operator: The smart contract itself is a participant in the sense that it facilitates and governs the lottery. It manages various functions, including ticket purchases, random selection of winner, and prize distribution. The smart contract also holds the funds collected from ticket sales and enforces the rules of the lottery.

Winner: These is a participant selected as winner based on the rules defined in the smart contract. Smart contracts typically use a random number generation algorithm to choose the winner in a fair and transparent manner.

These three parties will cooperate in the smart contract ecosystem to create a decentralized, transparent lottery system. Players buy tickets, the smart contract manages the lottery process, and randomness is provided in the selection of the winner. The smart contract code defines the rules and logic of the lottery and ensures that the lottery operates fairly and autonomously.

III. Functionalities

Ticket Purchase and Entry:

- Participants can interact with the smart contract to purchase lottery tickets.
- Each ticket (1 ether) purchase represents an entry into the lottery. No limited entry.
- The smart contract should validate ticket purchases, including checking that participants send the correct amount of cryptocurrency to participate and have enough gas fee to transfer it.
- It maintains a record of participants and their entries by a list of addresses.

Random Winner Selection:

- The smart contract includes a mechanism to randomly select one winner from the pool of participants every 15 minutes or the lottery closed by the Operator.
- Once the winner is selected, the contract should prevent further ticket purchases and prepare for prize distribution.

Prize Distribution:

- After the winner is determined, the smart contract automatically distributes the lottery prize to the winning participant.

- It ensures that the prize distribution process is transparent and verifiable, allowing the participant to confirm that he/she received the prize.
- Reset the list of address after the prize is distributed to the winner.

IV. Pseudo code

Functionality 1: Ticket Purchase and Entry

```
// Pseudo Code
If payment is received and is correct ticket price:
    Record the participant and their entry by address in an array
    Increase the prize pool
Else:
    Tell the participant that the payment is not received or the fund in the account is not enough
```

Functionality 2: Random Winner Selection

```
// Pseudo Code
If the lottery is closed:
    Generate a random number
    Determine the winner based on the random number of the list of participants
Else:
    Tell that the lottery is still open
```

Functionality 3: Prize Distribution

```
// Pseudo Code
If prizes have not been distributed:
    Give the entire prize to the winner's address
    Mark prizes as distributed
    Reset the array of participants
Else:
    Tell that prizes have already been distributed
```

V. References

- "Introduction to Smart Contracts." Ethereum.Org, ethereum.org/en/developers/docs/smart-contracts/. Accessed 25 Sept. 2023.
- Ybm. "Lottery Dapp -Solidity Smart Contract Breakdown." Medium, Coinmonks, 31 May 2022, medium.com/coinmonks/lottery-dapp-solidity-smart-contract-breakdown-6f67e50739a3.
- Hussain, Sajjad. "Smart Contracts in Simple Words and with Pseudo Code." Medium, Geek Culture, 26 May 2021, medium.com/geekculture/smart-contracts-in-simple-words-and-pseudo-code-c53240d78c4a.