**INFO 7500 Cryptocurrency/Smart Contract Final Project**

**Online Betting System based on Blockchain**

1. **Group Member**

Jian Min 001491533

Mibin Zhu 001424937

Mingyu Liu 001498402

1. **Introduction**

Nowadays, the gambling industry has gradually became legalized, no matter on offline or online. More and more people are pursuing the high returns from gambling and enjoy the fun from the high risk. But there still have some problem in this industy, not all the gambling platform can be trusted, some platform may take your money and gone, you have no way to find them. To sovle this problem, we came up with the idea of using the blockchain technology.

1. **Justification**

There have some problems for recent gambling industry, which is the reason why we need to make this blockchain system.

1. **User authenticity is uncertain**

When we participated in an online gambling or sports lotter, we do not know whether the opponent is a real user, maybe ‘he’ is just a robot set on the platform.

1. **Fairness**

One of the most difficult problem facing online gambling is the issue of fairness. Online gambling systems are implemented through code functions. Players do not use real poker cards in gambling games, but use simulated code to deal with this problem. Developers are free to modify the code in the system to achieve the role of operating the game.

1. **Safety issues of money**

Online gambling companies often need to use an online platform as an intermediate platform. When users enter the platform, they need to recharge virtual currency. When they leave, they use virtual currency to exchange real money. In this process, the most critical role is the platform, while the entry and the exit of money need to be operated through the platform.

But the flow of money is controlled by the local government, and some policies do not allow users to withdraw funds in some conditions. The inflow of funds is more secure than the outflow, but there still have some problems such as small platforms may directly blocking accounts and causing economic losses to users.

1. **International payment issues**

In some global online gambling platforms, cross-border payments are still difficult to solve. While the digital currencies in blockchain systems are not affected by national borders.

1. **User privacy issues**

When users login to their online gambling account, some personal information is necessary, such as name and ID number for checking information, contact information and email address to send notifications, their bank card information for fund transactions. All of these information should be protected to a certain extent, and if any of them is wrong, the user's personal information will be leaked.

1. **Aims**

When we write a contract using blockchain technology, we can achieve the following aims and advantages.

1. **Blockchain‘s transparency and anonymity**

Users login to their account with a private key. This private key matches a unique address, and users can track the ins and outs of their assets through this address.

1. **Fairness of the blockchain**

Blockchain technology makes online gambling platforms with the opportunity to prove their 100% honesty, completely changing the old habits of fraud. This technology can record all the gambling information and funding this information on the blockchain. It can be publicly disclosed on the entire network and cannot be tampered with. It avoids black-box operations and eliminates the possibility of shady manipulation.

1. **Blockchain supports global payments**

The cryptocurrency built on the blockchain is fully virtualized. Cross-border payments can be realized in the system without exchange, which is equivalent to the inherent world currency.

1. **Blockchain technology is anonymous**

Blockchain technology greatly protects the privacy of individuals through mathematical encryption, and users' assets on the blockchain will be extremely secure.

1. **Methodology**
2. **Solidity**

Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum. It was developed by Christian Reitwiessner and several former Ethereum core contributors to enable writing smart contracts on blockchain platforms such as Ethereum.

1. **React**

React is a JavaScript library for building user interfaces. It is maintained by Facebook and a community of individual developers and companies.

React can be used as a base in the development of single-page or mobile applications. However, React is only concerned with rendering data to the DOM, and so creating React applications usually requires the use of additional libraries for state management and routing.

1. **Truffle Suite**

A world class development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine, aiming to make life as a developer easier. With Truffle, you get: Built-in smart contract compilation, linking, deployment and binary management; Automated contract testing for rapid development; Scriptable, extensible deployment & migrations framework and so on.

1. **Implementation**

**Simulation of the lottery purchase process**

Firstly, suppose there have three people A, B and C in this system. Where A is a manager role, the duty of A is just for clicking the “Settlement” button in this process. User B and C are the buyers of the lottery, they may have competition with each other to guess the number for being the winner.

This system is still a decentralized system, cause we have contracts between A & B and A & C. For each contract, only when two of them sign their name to say “yes” we agreed on this, which means they both agree to send their money to the contact, then the contract will work. After the betting is over, the contract will send all the money to the winner and finish the contract to get ready for the next lottery.

Secondly, we look back to the lottery purchase process. For each time, the buyer enters the number he wants to buy in the input text (we suppose the number is between 1 to 100). Each purchase will cost 1 ETH and 0.03 GAS, and after they decided what to buy, they can click the “Bet” button for confirm. The buyers can buy multiple times and the upper limit is 99, cause we don’t want to make the lottery process meaningless. And on the other hand, different people can buy the same number of the lottery, if they both win, they can share the money with the percentage of what they pay for that number.

Finally, when manager A clicks the “Settlement” button, a number will be generated by the system by default, and then this number is compared with the lottery number which are bought by the users. We may have following 3 conditions:

1. Condition 1, only one person guessed correctly, then the money will be given to that person depended on the contract.
2. Condition 2, if more than one person guessed correctly, the money will be distributed to each person, while the percentage will depend on the amount they are betting for.
3. Condition 3, If no one guessed right, the contract will return the money to each person in the betting system.
4. **References**
5. **Solidity definition :** [**https://en.wikipedia.org/wiki/Solidity**](https://en.wikipedia.org/wiki/Solidity)
6. **Solidity develop :** [**https://solidity.readthedocs.io/en/develop/**](https://solidity.readthedocs.io/en/develop/)
7. **React definition :** [**https://en.wikipedia.org/wiki/React\_(web\_framework)**](https://en.wikipedia.org/wiki/React_(web_framework))
8. **Truffle suite :** [**https://www.trufflesuite.com/docs/truffle/testing/writing-tests-in-solidity**](https://www.trufflesuite.com/docs/truffle/testing/writing-tests-in-solidity)