Construction Method of Casino based on Ethereum

Jianzhi Rong *

Mathematics, University of California, Santa Barbara, California, US

* Corresponding author email: Rong@ucsb.edu

Abstract. There are a lot of things that humans cannot do, and one of them is being fair, especially when he is running a casino. However, Ethereum can. Constructing a casino that is regulated by Ethereum can give us the first fair casino in the world. With the help of some technics of cryptography, which are public/secret key schemes and one-way functions, the secrecy and privacy in the gambling of each player can be ensured while still making the game fair by the blockchain. During the construction, Ethereum is also found to be fit for the casino's other aspects such as propaganda and payment. By successfully constructing such a casino, a way of converting the fixity of blockchain into fairness is proposed in the area that needs it and lacks it the most, which is a casino. Following down this road, any area that lacks fairness can exploit Ethereum or block-chain to find a way to achieve fairness.

Keywords: Blockchain; Ethereum; Fairness.

1. Introduction

A casino, by definition, is a place where gamblers can play games with their luck [1]. Good tactics can raise the rate of winning money for a gambler, but the decisive element of the games need to be pure luck so that a beginner still has a chance to win the money from a veteran [2]. However, there is no such casino. As long as the casino is held in people's hands, the game will then be between the gambler and the whole casino. There are so many ways that a casino can make the game of gambling unfair. In this era of high technology, any seemingly normal card in a casino can be secretly marked or modified. If the casino is physical, then any people in it can be misleading informers or corrupt players [3]. For some casinos, gamblers cannot even walk out the door with their winning money. Even though there is one such fair casino in Las Vegas, the distance to Las Vegas can still block most gamblers all over the world. That is why to construct a casino based on Ethereum, which is to welcome gamblers from the whole world with a fair casino. Let the gambles be held by Ethereum's public ledger can make sure the gambles be fair since the generated public ledger is no longer changeable. This Ethereum casino also has all the advantages of usual online casinos. First, it does not need regulations of physical employees, sites, and security. Second, it also guarantees the gamblers' physical security [4]. Third, the distance barrier is also dissolved. Last but not least, the propagation will be easier by, for example, inserting into popular websites. In addition, compared to the usual online casino, Ethereum casino is also easier to survive. Since Ethereum is decentralized which means that there is no regulation of any entity, most legal issues can be circumvented. In this paper, a way of constructing a fair Ethereum casino is going to be proposed.

2. Associated Technology

2.1 Why Ethereum

2.1.1 Block-Chain

The reason to build the casino above Ethereum is that the only way to achieve fairness of the casino is to utilize the blockchain of Ethereum [5, 6]. Blockchain is a chain of timely ordered blocks of messages, which is also called the public ledger of Ethereum. Rather than stored in one place, this whole chain is stored in all the nodes all over the world at the same time, which means that all the information of the whole Ethereum platform is shared by every node, and anyone can become a node by downloading the related Ethereum clients. If any of the messages of Ethereum need to be changed, it has to be agreed by the majority and the whole chain stored in the whole world will change so that there is no single party or entity that can change any messages in Ethereum. As a result, Ethereum become a decentralized platform, in another word, it is not regulated. In addition, anything that is already in the previously constructed blocks can no longer be modified and this is actually how the casino is going to avoid cheating.

2.1.2 Why not Bitcoin

Ethereum is not the only one that is using the block-chain. In fact, Ethereum learned the block-chain from Bitcoin which invented this block-chain at first. However, the block-chain of Bitcoin is not as good as the block-chain of Ethereum for constructing a casino [7]. Consensus algorithm is the way how do a block-chain build new blocks. The consensus algorithm used by Bitcoin is Proof of Work (POW) [8], while Ethereum is Proof of Stake (POS) [9]. First of all, Ethereum is more efficient. By POS, for every 12 seconds which is a slot, there is going to be a new block. However, for POW, creating a new block need to hash millions of times and the system will continue to raise the difficulty to ensure the value of bitcoin would not depreciate too soon. As a result, every block of bitcoin is created approximately every 10 minutes. This is bad for running a casino because it would take too long to run a turn of gamble. Second, POS is more economically safe for a casino because due to POS, for becoming a possible attacker there is a stake of 32 ETH, which means that attack a gamble would spend much more than the whole value of the gamble.

2.2 Public Key and Secret Key Scheme

The public key and the secret key scheme are the foundation of cryptography and cryptocurrency. The basic idea is that the raw message needs to be transformed secretly between the sender and the receiver across the Internet and these two keys are going to help them achieve this goal. The public key is used by the sender to encrypt the raw message, the encrypted message is sent over the Internet to the receiver and the receiver is using the secret key that is only known to himself to decrypt the message so that only the sender and the receiver know the raw message. For every account of Ethereum, there is already a secret key associated with the address combined with the account as long as it is created.

2.3 One-way Function

A one-way function is a type of function such that given the output and the function, you cannot calculate the input. In other words, the function is not invertible. In cryptography, the one-way function plays a big role in storing passwords. By storing only, the output of the passwords from a one-way function, even if the website is attacked, the attacker can only see the output and the one-way function and still have no idea of the password. The most common one-way functions are MD5, SHA, MAC, and CRC.

3. Construction of the Casino

3.1 Propaganda

When the casino is completely constructed and tested functioning, it will appear on the App part of the website of Ethereum. All the users of Ethereum then can see the casino which means that all the propaganda and refinements of Ethereum are also bringing potential customers to the casino. Since Ethereum is the largest decentralized platform and has more and more people joining in from all over the world, propaganda would not be a problem at all. The good point is that on Ethereum there is no source of messages because of the blockchain so disseminating the information of the casino is facing no legal issues or scrutiny.

3.2 Gamble

There are thousands of games and thousands of versions of games that can be played in a casino, but all the underlying elements are similar. In this part, the execution of Texas Holds 'em poker is going to be an example of how any game can be played fairly in the Ethereum casino by block-chain [10].

Texas Hold'em is played usually between two to ten people with a deck of cards. Each player will be given one card at a time until they got two cards and these two cards are only known to them. Then there will also be five random cards from the same deck on the table while three of them are opened and the other two are going to be opened each betting round. The ultimate goal is to combine the two cards at hand with the five cards on the table to have the max combo of five cards. Each player after seeing their two cards can choose to raise the bet if there is already a good combo combining their two cards with the three open cards on the table, to just keep up to see if they can get a better combo after flipping the other two cards on the table or to discard their cards with no punishment.

3.3 Auto-Dealer

First of all, the two cards for each player and the five cards on the table need to be totally random. For any physical casino, cards could be marked in any technological way or the dealer could use their gimmick to sequence the deck as they want, but in the Ethereum casino, cards would be randomly assigned by the auto-dealer. At the beginning of the game, the program auto-dealer would shuffle the listing deck with those 52 cards as elements. Then, the auto-dealer would assign two cards to each player once at a time and put five cards on the screen with three cards open and the other two closed. However, at this point, the auto-dealer has not actually sent the cards to the players. The auto-dealer will need to first randomly generate four One-Way Functions for the four suits of the cards accordingly. Then, the auto-dealer will input all the best cards in the deck beside the cards for the players and the cards on the table accordingly with their suits, and put all the results from the rest cards on the screen. In this way, all the rest cards of the deck have been fixed by recording their results of one-way functions in the blockchain so that neither the casino nor the players can change the cards to cheat. At the end of the game, the four one-way functions for the four suits of the cards will be published to everyone so that every player can also check that all the cards can match the results to constitute a complete deck. In addition, those results from one-way functions also have no clues to the cards in other players' hands. First, all four one-way functions are only published at the end of the game and are randomly generated each time so that each player cannot know the input while they only have the output and do not know the function. Second, using a one-way function also raise the difficulty of calculating the inputs. Third, even though all the results of the rest deck are calculated, as long as there are more than two players or the cards on the table are not opened, the cards in other players' hands are still unknown.

Second, the two cards for each player need to be secretly known to only themselves. After assigning the cards and finishing putting all the Hash results on the screen, the auto-dealer will start to encrypt the two cards for each player with their own public key associated with their address of Ethereum accordingly. That is why the dealer need to be automatic so that nobody in this world but themselves know their two cards at hands. Even though all the other players are collaborating, there are still remaining cards in the deck so that they can still not know the cards of the honest player. Then the encrypted two cards will be sent over the Ethereum to each player and they can decrypt the two cards by their secret key. Then the betting round can start as usual until the end. In addition, since the casino is using the public key and secret key of Ethereum directly, any update of Ethereum would benefit the casino directly by raising the difficulty of attack the private cards of each player.

3.4 Payment System

For every betting round, players can directly use Ether to bet so that there is no need to buy tokens. In addition, there are already many well-developed loaning Apps on Ethereum, like Oasis and PWN, so that the casino can also collaborate with them to help players to pay. Players can even negotiate with each other to sign contract like 100 of the future mined ETH of one player will be sent to the other player [11]. The payment method is every mutable in Ethereum, and the good point is that mutable payment method can avoid legal issues. For example, the previous contract about one player mining for the other player will not be defined as trade of belongings, and staying away from legal issues can bring gamblers from more areas.

4. Conclusion

By utilizing the decentralized blockchain of Ethereum, combined with a one-way function and public and secret key scheme, a way of constructing a fair online casino on Ethereum is formulated. To make the gambles fair, first of all, both the casino and the players need to be unable to manipulate the gamble so that letting the decentralized Ethereum control the gambles by fixing all the cards in its unchangeable blockchain can achieve this goal. By automatically storing all the associated cards into a blockchain before every gamble start, the result of each game can be verified after each gamble ended, and making the storing process automatic can avoid any manipulation. The second step to fairness is to maintain secrecy among all the players. In the process of showing all the cards have been stored in the blockchain, there is a danger to leak information about the cards that are going to be stored and fixed. With the help of encryption of a one-way function, the danger of exposing the cards to players can be avoided by only showing the encrypted output of those stored cards to the players. In the process of sending each player their own cards, there is also the danger that these private cards could be attacked and stolen. With the help of the public and secret key scheme of Ethereum itself, the privacy of each player against the rest of the Internet is also ensured. In addition, the propaganda of Ethereum can help to propagate the casino, and payment on Ethereum can also be made in many ways. As a result, an Ethereum casino is totally feasible. However, the safety of the player is still not perfectly ensured. All the usable one-way functions are there, which means that there is a chance that all the randomly generated four one-way functions are occasionally guessed correctly by the attacker. At the same time, all the other players need to all collaborate with the attacker so that they can calculate out the hand cards of the last honest player. However, the attacker can still not manipulate the cards but can only know the cards. All in all, this attempt to construct an Ethereum casino is to find a way to construct the first proven fair casino in this world. With the help of some technics in cryptography, we take advantage of the property of decentralization and fixity of the blockchain of Ethereum to achieve fairness in a casino, which is a place that needs it and lacks it the most. In this logic, any area that needs more fairness can utilize the blockchain of Ethereum. For example, in the desire for a fair boss, decentralized autonomous organization (DAO) is the most discussed topic about block-chain in 2022. In the version of AI, the blockchain can also act as the memory of a needed justice authority or even a major.

References

[1] Bradley G T, Wang W. Development and validation of a casino service quality scale: A holistic approach[J]. Tourism Management, 2022, 88: 104419.

[2] Huang L, Liu M T. Backfires on firms' intangible assets of the casino industry in Macau and Las Vegas: investigating advertising expenditure[J]. Asia Pacific Journal of Marketing and Logistics, 2021.

[3] Zhou Y. COMPARATIVE LAW OF ONLINE GAMBLING–LEGAL AND TAX FRAMEWORK[D]. Universidade de Coimbra, 2021.

[4] Firmansyah Y, Haryanto I, Purnama T A, et al. Compensation for Fraud (Gambling) Operations Under The Guise of Investment–Restitution as a Complex or Easy Way Out Mechanism?(Learning from Various Restitution and Law Cases in Indonesia)[J]. East Asian Journal of Multidisciplinary Research, 2022, 1(3): 545-572.

[5] Kumar K K, Karimunnisa S, Krishna A, et al. An advanced approach for Smart Parking Solution Based on Ethereum Block chain System[C]//2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2021: 942-948.

[6] Harshitha M S, Shashidhar R, Roopa M. Block chain based agricultural supply chain-A review[J]. Global Transitions Proceedings, 2021, 2(2): 220-226.

[7] Gurman Singh Kohli D, Sharma M, Shanker S. Block Chain Technology and Its Impact in the Business Environment[J].

[8] Milunovich G. Assessing the connectedness between Proof of Work and Proof of Stake/Other digital coins [J]. Economics Letters, 2022, 211: 110243.

[9] Saad M, Qin Z, Ren K, et al. e-pos: Making proof-of-stake decentralized and fair[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(8): 1961-1973.

[10] Xu J, Chen J, Chen S. Efficient Opponent Exploitation in No-Limit Texas Hold'em Poker: A Neuroevolutionary Method Combined with Reinforcement Learning[J]. Electronics, 2021, 10(17): 2087.

[11] Mohammed A H, Abdulateef A A, Abdulateef I A. Hyperledger, ethereum and blockchain technology: A short overview[C]//2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2021: 1-6.