BSCDL: A Blockchain based Smart Contract Digitized Lottery Scheme

Aditya Vajpayee Aditya Tomar Shivam Singhal

March 19, 2020

BSCDL: A Blockchain based Smart Contract Digitized Lottery Scheme

Aditya Vajpayee , Aditya Tomar ,Shivam Singhal

Department of Electronic Communication Galgotias College of Engineering and Technology.
Greater Noida, India
Department of Electronic Communication Galgotias College of Engineering and Technology. .
Greater Noida, India
Department of Computer Application,Cochin University College of Engineering,kuttanad.
Kerala, India

Abstract

This research is based on generating the lottery system software. The existing system of lottery is done manually in a majority. Thus in this computerized and technological world there is an urgent need for the improvement of the lottery system also. Thus introduces a novel approach for developing a software for lottery system using blockchain which is one of the most security granted, decentralized technology. It includes the selling, purchasing, declaration of result . Here the randomness and fairness of declaring result is ensured and thereby providing a tamper-resistant, transparent and efficient system. Here we introduce a smart contract based system that include registration, purchasing, prize declaration, lottery claiming, and payouts. This paper put forth a blueprint of a novel lottery system hinged on Blockchain technology, that coalesce lottery operations models and blockchain mechanisms.

1 Introduction

Blockchain has been emerging as one of the vital technology influencing our day-to-day life. Blockchain is a neoteric financial-related technology which is actually a database comprising of data structures that allows to make records in a secure and transparent way and the verification of any type of transaction in a decentralized manner. Each block in a blockchain have Data, Hash and Previous Hash which avoids forging of datas, piercing into the system etc., As it becomes preposterous since data is stored and disseminated in a copy on everyone's m achine and also the act of linking blocks makes the data stored on the Blockchain trustworthy. A pivotal characteristic of Blockchain is the considerable use of cryptography which is used as a linking element between blocks that helps to bring authoritiveness behind all the interactions in the Blockchain.

Lottery games are different from other gambling games because these games doesn't depend upon the skill of the player but is completely depended upon the luckiness. There is an urgent need for replacement of traditional system by a totally computerised system that ensure fairness, transparency and the fair distribution of funds, which all are the most common problems that most people surmise, distrust, and complain about .

In Lottery game, the winning factor is determined merely by chance with no prowess involved[2]. Lottery players are not classic gamblers. Lottery players are investing a small sum of money for buying a dream to be an instant millionaire which is completely depended upon the chance,hoping to thrive it and possibly win a life-changing prize. Each participant buys a ticket expecting for a dream to be fulfilled.

In the current system we have intermediaries and merchants to sell lotteries to people in each area. Also the remaining processes like auditing and declaration of results are done by intermediaries manually under subjugation of the government. With this system the people are concerned about unpredictability and uniformity, they are also concerned with the fairness, verifiability and tamper-resistance of the random numbers.

And due to these facts we bestrew Blockchain with the process of purchasing and selling of lotteries. We use blockchain technology in evaluating payment, ticketing and payouts in distribution environments.Blockchain network allows equal participation of each player. There is no central power concept instead power is distributed among all participants.

The process of lottery includes certain phases that is Registration, purchasing, closing, verifying, random selection of winners, Winner announcement and payouts. Security in payments, ticketing and payouts in distribution environments is ensured in the system using blockchain.

2 Innovtive 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] , was launched in 2015. Ethereum supports the execution of smart contracts. Ethereum is a blockchain based open platform which is able to provide developers with the capability to build and deploy a decentralized application. It is one of the key concept which are small computer program that “live” in the Blockchain. It is a piece of code that runs on blockchain.

Blockchain technology was limited to the fields of financial operations but now with the emergence of smart-contract extends the fame of blockchain technology to many other areas such as lottery. Smart contracts in blockchain allows the developer to program thier own applications without the need for any transition in the blockchain, thus improving the scalability of blockchain.

2.1 Blockchain

Blockchain is a distributed ledger technology. It is an imperishable digital ledger of economic transaction. In blockchain it allows to record not only financial transactions but virtually everything of value. It is a structure consisting of blocks that stores transactional records, of several heterogeous records in several databases, which is known as the “chain,” in a network connected through compeer-to-compeer nodes. Generally, this storage is referred to as a 'digital ledger’. This allows digital information to be rationed, but not transcribed. That means each individual piece of data can only have one owner and also the deed of associating blocks into a chain makes the information stored on blockchain trustworthy.

Blockchain is a distributed database providing a secure, transparent and a decentralized way of making, recording and verifying any type of transactions. Blockchain eradicates the requirement of a centralized control by making all transactions decentralized, and verification is done by the blockchain database itself in the distributed ledger.

Blockchain is comprised of three core parts are : block, chain, and network. A block records a list of transactions into a ledger over a given period of time. A chain is a hash linking one block to another. Data from the previous block is used to create the hash and it is a dactylogram of the data and clamps blocks in order and time. A network is an association of nodes. Each node contains a plenary record of all the transactions that were ever recorded in the associated blockchains. Operating a node is expensive and time-consuming.

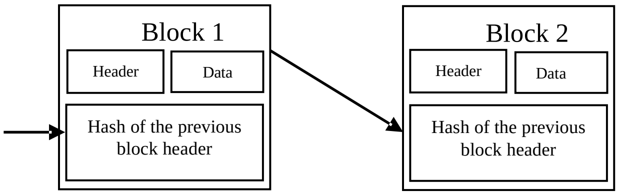
Block 1
Header
Data
Hash of the previous block header
Block 2
Header
Data
Hash of the previous block header

Figure 1: Structure of Blockchain

2.2 Ethereum

Ethereum was launched in 2015. Ethereum is an open source, prominent, public, distributed and blockchain-based computing platform highlighting smart contract functionality. The Ethereum is currently the most appropriate one to build decentralized applications. Ethereum is a blockchain based open source pulpit which is capable of providing developers the ability to build and set-up a decentralized application. Ethereum is a platform betrothed to grant people to conveniently write decentralized applications using blockchain technology. In Ethereum blockchain, prospector endeavour to earn Ether,which is a type of crypto token which fuels the network. Ethereum is a pulpit for sharing information across the globe that cannot be wielded or altered. Ether also known as ETH is a decentralized digital currency.

2.3 Smart Contract

In simple words Smart Contracts are small computer programs that “live” in the blockchain or runs on blockchain. The emanation of smart contract makes blockchain not only applicable to the financial fields, but also other fields, such as lottery. It is an agreement between two people in the form of computer code. Smart Contracts runs on blockchain, and hence stored on a public database and cannot be altered. The transactions that occur in a smart contract are handled by the blockchain, that is they can be sent automatically without a third party. Ethereum is a decentralized computing platform which spawns a crytocurrency token which is known as Ether. Smart contracts are executed automatically based on the code that the programmers program on Ethereum Blockchain. Ethereum Virtual Machine are used for running these contracts which is composed of all devices running on Ethereum nodes. The “decentralized platform” part means that anyone can set up and run an Ethereum node by paying the operators of those nodes in Ether, which is a cryptocurrency token tied to Ethereum. Thus, computing power is provided to the people who run Ether and are paid in Ether.

2.4 Verifiable Random Function

A verifiable random function (VRF) is a spurious-random function.When we provide an input x to a VRF it produces a random number y along with a proof z for y. With the help of z, every participant can verify whether y was generated correctly from x or not. A VRF is the public-key version of the keyed-cryptographic hash. In VRF, only the one with the private key can compute the hash but anyone having the public key can verify its definiteness which is clear that it is unlike the the normal hash functions. A VRF also has to placate the following properties:

(1) Uniqueness: When an input x is given, there should be a unique y, such that the verification returns true.

(2) Provability : if x generates(y,z), then the verification returns true.

(3) Pseudo-Randomness: In case of a uniform distribution, the output y should be indistinguishble.

3 Design and Related Works

Everything around us are emerging in a great way with the invention of technologies and are getting computerized in massive way. Depending on this revolution there is a urgent need for improvement of lottery system which is one of the perennial games existing today also. For this purpose we introduce a smarter way of playing lottery games which is fully computerized, decentralized and is implemented effectively through Blockchain technology.

3.1 Overview

User registers into the system, purchases a digital lottery by paying amount and the wait for the result. The result is randomly declared . User can check for his prize and if won he can claim for the prize and the won amount will be transferred to his account. If the user fails to check for the result then also the result notification and won amount will be transferred to his account based on the earlier registration.

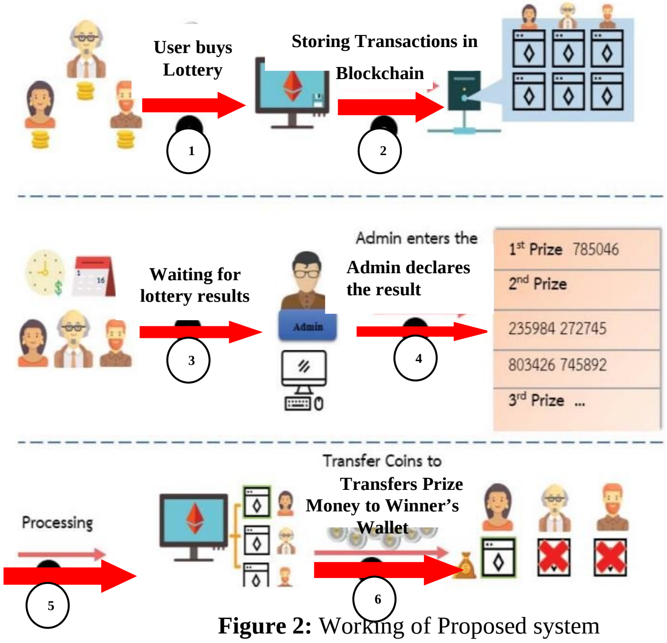

Figure 2: Working of Proposed system

3.2 System Goals

The goal of the system is to design a fair and an efficient lottery scheme, which ensures the integrity and legitimacy of lottery result and is public to all the participants.

(1) Random Number Generation : Since the winning number is predicted randomly it is assured for the accuracy of the result, since none of the players or the lottery centre can predict the value of winning number .

(2) Public Verification : All stages in this system are put public so that all people could verify for the fairness of the lottery.

(3) Efficiency : This system is a fully efficient one, which means the players can buy lottery tickets adroitly and fairness of the lottery is verified rapidly.

3.3 Workflow

Initially, address of Ethereum will be provided to the buyer for the purpose of purchasing the lottery.This is done by providing a sign-in page for the buyer through the website where he will be registered. After the registration and attaining the address, the transaction will begin. The buyer is then able to purchase the ticket by using the address and he can select the desired number from the given set. Consequently, the system will calculate the price and they have to pay the amount. Once the purchasing process is done, the transaction will be recorded to the blockchain. The system will retrieve all of the lottery tickets that are purchased and sold and scrutinize those series to determine the reward. When the result is ready to be announced the Lottery Administrator publishes the winners list, which will be then filled into the result page. If a customer won a reward, the system will calculate the amount of the reward in proportion of the sale amount and transfer it to winner's wallet.

3.4 Operation Performed

When a customer purchase a lottery for the first time they have to register and the system will assign them with an Ethereum address. After registration, customer can choose from a set of tickets available and pay the prerequisite amount and purchase the digital lottery.And each of these transactions will be parallely stored into blockchain. Then required datas will be retrieved from blockchain stored in the database which is then transferred for the trade to occur. If it is a purchase for the first time, the system will add new Address and new Number of customers to database.

3.5 Determintion of winners and award announcement

A set of lottery tickets will be generated in a certain range of series.The determination of result depends on the number of the lottery ticket series purchased in each set per one address by Lottery Administrator. Then he performs random number generating function and thus determines the result and thus announces the winners. After publishing the results winners can claim the prize which will be then automatically rewarded in their wallets. Thus it provides a valid and user-friendly approach compared to existing system.

4 Benefits

The proposed model of blockchain based lottery system have several benefits:

1. User need not keep any paper or ticket since there is a great chance of missing, getting ruined, also blemishing of the Barcode on the ticket which all will lead to the rejection of his prize.

2. Since the user buys ticket by registration the digitalized ticket is safe in his custody and thus prevents any false claimant.

3. User gets a chance to select from a available list of series number of that day.

4. Each prize will be generated step by step and live that is, it takes less than 1 minute to complete the drawing of lottery for a particular day.

5. Software automatically deposits the cash on winner’s wallet, thus elucidating the dilemma of winner’s missing of checking the prize.

6. Each lottery result will be store on the block chain as hash values. Thus ensuring security.

7. User can search for a previous date of draw of lotteries and view the results.

In addition to these, by using blockchain which provides decentralized approach there are certain more properties that are desirable:

1. Unpredictability: no one should be able to compute the winning number or predcit the random values.

2. Tamper-Resistance: no one should be able to mold the result and thus yield benefits from the outcome.

3. Unbiasibility: Any colluding adversary or even a single party should not be able to influence future random values to their convenience.

4. Public-Verfiability: Any external verifier should be able to verify generated values using public information only.

5 Security Analysis

5.1 Prediction Attack

This attack is related with the pecomputing and prediction of results by players or lottery centres. If this can be done, then they can buy the ticket that is bound to win, which makes the lottery results skeptical. All theses issues are efficiently solved with the use of Blockchain.

5.2 Bias Attack

Biasing the choice of winning number is another major attack done by lottery centre for achieving their different goals which all causes a violation in the fairness of lottery. This can be done by trying to pick up the winning number that no player has chosen or by picking up a winning number that matches a ticket that a specific user bought.

5.3 Forging Attack

After the declaration of result, a player other than the winner or the lottery centre may try to forge a winning ticket.

5.4 Impersonating Attack

After the winner is announced, sometimes there is a chance that another user may try to impersonate and thus accept the award. But here, anyone cannot pretend to accept an award. Because a player inititates a transaction on blockchain every time when executing a smart contract. Blockchain comprises of a perfect signature mechanism, where every transaction includes initiator’s signature, making it impossible for others to fake.

6 Analysis

In this paper it is discussed about digitizing the processes carried out throughtout a lottery scheme by using Ethereum Blockchain.Thus it rectifies the issues encountered in the exisiting lottery system.

This system allows the customer to purchase the lottery without relying on intermediary thus proceeding to payment and buying of a digitized lottery, as well as, the user can track ev ents online as well claiming prizes through the system itself. From the intial process till the end everything is done virtually on Blockchain. This system emulates the present system with the additional features of providing transparency in purchasing and selling, tracking each deals at a particular span and a secure transmission of prize amount to winner’s wallet.

7 Conclusion

This paper introduces a new methodology using Blockchain and Ethereum network in the process of selling and purchasing of lottery . This system will replace the original lottery operations in every aspect such as the removal of third-parties in buying process, ensuring the efficiency in prize declaration and the claiming of prize. The winner number can be generated through traditional random number generator. Firstly, every player are provided with the whole set of series available, from which they could choose.Secondly, it provides a secure gateway for purchasing.Third, the result could be verified publicly by all the player. Fourth, claiming of prizes is easy and finally the transfer of prize money to winner's wallet which is done automatically.Each records regarding the purchase will be stored on blockchain and also the prize details and thus provides a verifibale and transparent system for the participants. Here we have mentioned all those attacks which are possible on the lottery system and have proposed an effective way to bulwark against those attacks through our scheme.

In general, this system can curtail almost every preeminent problem of the traditional lottery and it ensure fairness to the consumer as well.

References

1. Liao, Da-Yin, and Xuehong Wang. (2017). *Design of a blockchain-based lottery system for smart cities applications*. 2017 IEEE 3rd InternationalConference on Collaboration and Internet Computing (CIC). IEEE,2017.
2. T. Barker and M. Britz. (2000). Jokers Wild: Leglized Gambling in the Twentyfirst Centuary, Praeger.
3. *The Ethereum Project*. (14 September2017). Retrieved from https://www.ethereum.org
4. Liao,Da-Yin and Xuehong Wang. (2018). *Applications of Blockchain Tech- in Integrated Casinos and Entertainment*. Informatics.ol.5.No.4. Multidisciplinary Digital Publishing Institute.
5. Wood, G. (2014). *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. Retrieved from: http://gavwood.com/paper.pdf
6. P. Kuacharoen. (2012). *Design and Implemetation of A Secure Online Lottery System* (pp. 94-105). IAIT.
7. V. Ariyabuddhiphongs. (2011). *Lottery Gambling: A Review*, Journal of Gambling Studies, vol. 27, no. 1,(pp. 15-33).