BanFEL: A Blockchain based Smart Contract for Fair and Efficient Lottery Scheme

1st Jiasheng Li
Beijing Engineering Research Center
of Massive Language Information
Processing and Cloud Computing Application
Beijing Institute of Technology
Beijing, China
jiashengli@bit.edu.cn

2nd Zijian Zhang
Beijing Engineering Research Center
of Massive Language Information
Processing and Cloud Computing Application
Beijing Institute of Technology
Beijing, China
School of Computer Science
University of Auckland
Aukland, New Zealand
zhangzijian@bit.edu.cn

3rd Meng Li
Key Laboratory of Knowledge Engineering with Big Data
(Hefei University of Technology)
Ministry of Education
School of Computer Science
and Information Engineering
Hefei University of Technology
Anhui, China
mengli.hfut@gmail.com

***Abstract*—Lottery is a game with many people's dreams. But corruptions of lottery centers make the lottery unfair. To address this unfair issue, fair lottery schemes have been studied for several years. In these schemes, delay functions or aggregation protocols can be used to generate the winning numbers fairly. However, to the best of our knowledge, none of the existing schemes can achieve the winning number generated randomly, while the randomness can be verified fairly. In this article, we first propose a [B]lockchain based sm[a]rt co[n]tract for [F]air and [E]fficient [L]ottery (BanFEL) scheme. We further present a winning number random generation smart contract, by which players submit the purchased numbers and the non-tampering property is protected. Security analysis and experiments show that the fairness of BanFEL is protected better than the existing works. Meanwhile, the verification cost of this scheme are at least 0.03s lower than the traditional Grumbach's scheme between 1000 and 10000 players.**

***Index Terms*—blockchain, fair lotteries, publicly verifiable lotteries.**

I. Introduction

Worldwide lottery sales totaled $3032 billion in 2017 [1]. However, there are many corruptions and unfairness in lottery industry all over the world.

In 2017, the director of information technology at the Iowa lottery company took advantage of his position to tamper the lottery center's random number generator and helped his friend win the first prize of the lottery, which worth $783,000 [2]. In the same year in China, the former director of the China welfare lottery distribution management center was put on trial for suspected serious disciplinary violations [3]. The corruption news and unfair stories are caused by the centralized lottery operation structure. Operator of lottery center may collude with parts of players, which will cause unfairness in lottery. It is necessary to weaken the power of lottery centers and make the process of lottery public to all the participants and can be verified fairly.

Blockchain and Secure Multi-Party Computation can be used to solve the problems in lottery. Blockchain is a decentralized public database based on consensus mechanism, which has the characteristics of decentralization, transparency and non-tampering. Every player can participate in the blockchain network equally. Power is not controlled by central institutions but is shared among all participants. SMC is widely used in electronic lottery, electronic auction, secret sharing and many other scenarios. Secure Multi-Party Computation(SMC) is a collaborative computing problem that addresses privacy protection in a group of untrusted participants without a trusted third party.

In recent years, several fair lottery schemes have been proposed. Specifically, Massimo et al. [4] proposed a lottery smart contract on Ethereum. However, the scheme compares all participants in pairs until a winner is produced, which results in low efficiency. Liao et al. [5]designed a blockchain-

This work is partially supported by National Key Research and Development Program of China (Grant NO.2016YFB0800301) and the National Natural Science Foundation of China (Grant NO.61772070).

978-1-7281-2319-6/19/$31.00 ©2019 IEEE

based lottery system, protects the irreversibility of buyers submitted lottery value, but the winning numbers of lottery still generated by the lottery center.

Also none of the existing work guarantees that the winning number is truly random, and the participants of lottery cannot verify the result of lottery. A fair and efficient lottery scheme is necessary to enhance players' confidence. On the one hand, the winning number is generated randomly and can be verified by all the participants rapidly. On the other hand, the purchase records of players cannot be modified maliciously. It is difficult to find out a random number generation algorithm and the randomness of the number can be verified easily. Another difficult is to protect the Non-tampering property of the players' purchasing records.

We proposed a BanFEL. The lottery center assigns the deadline of purchasing and the deadline of opening that represents the end time of players sending commitment and opening the commitment. Players send the commitment of ticket values before the deadline of purchasing, and open the commitment between the deadline of purchasing and the deadline of opening. In this case, even if a player becomes the last one to submit ticket values, he do not know others' ticket value, so he cannot finish SMC. After all the commitments are opened, lottery center can calculate the winning number by SMC and select the winners. The contributions of the scheme are summarized as follows.

1) We propose a winning numbers generation method of the lottery, which ensures that the numbers are truly random. Simultaneously, all the participants can verify the randomness of the winning numbers rapidly.
2) We design a smart contract, by which players can submit their purchasing request, and the records are tamper-resistant.
3) The experimental and security analyses are performed to verify the efficiency and security of the scheme.

II. Related Work

A series of researches on smart contract and distributed lottery protocol has been proposed in recent years.

A. Smart Contract

A blockchain platform, Ethereum [6], was proposed in 2014. Ethereum supports the execution of smart contracts, which is programmed by a Solidity program. Smart contracts improves scalability of blockchain, which means that the developer can program their own applications without the change of blockchain. In recent years, many kinds of application based on smart contract have been proposed, such as electricity transaction , authority management in Internet of things(IOT) [7] and medical data access [8].

Sikorski [9] presented a scenario includes two electricity producers and one electricity consumer trading with each other over a blockchain. The distributed ledger provides all participants with realistic data produced by process flow sheet models, which means the transactions transparent to all the people. Azaria [8] proposed MedRec, which is a novel,decentralized record management system to handle electronic medical records(EMRs) bu using blockchain technology. EMRs are sensitive data, MedRec ensures the confidentiality, accountability and security sharing of it.

But there is a drawback of smart contracts that it is prone to privacy leakage. Hawk, a model of smart contract, was proposed in 2016, compile the smart contract into a public part and a private part and the privacy of users are preserved when executing the smart contract. There are many schemes based on Hawk model has been proposed.

Christidis [10] demonstrated whether the blockchain make a good fit for the IOT sector. First, blockchain promotes the sharing of services and resources in the IOT, leading to the creation of a marketplace of services between devices. Second, smart contract allows us to maintain a time-consuming workflows automatically in the IOT. Peters [11] provided an overview of blockchain's potential to disrupt the world of banking through facilitating global money remittance, and discussed the issues of developing such ledger based technologies in a banking context, which must be considered.

B. Distributed lottery protocol

The potential of the Bitcoin blockchain [12]for a distributed random process has been examined. There has been some lottery schemes based on blockchain has proposed but most of them focus on the payment [13], Collateral [14] and other aspects of the lottery. However, it has been shown that the manipulation of presumably random bits is realistic even with limited computational capacity and financial resources [15]. An integration of the proof of work from [16] and an alternative crypto-currency Ethereum [6] has been proposed with no practical solution yet for a verification due to the limitation imposed by the blockchain. There are some researches that designed distributed lottery schemes with the thinking of blockchain.

Grumbach et al. [17] propose a distributed aggregation protocol for a large scale peer-to-peer lottery. It uses a data structure, merkle tree, to generate the winning number of the lottery. Every player is a leaf of the merkle tree, the location of which is stipulated by the lottery center. Then, all the players calculate the root of merkle tree together, and solve the Byzantine General Problem to get a real number that generated by most of honest players. Though the winning number is generated by all players rather than the lottery center. But it also has the limitation that only one lottery tickets can be bought per players. And some security problems still exist in the scheme. What matters most is the efficient of the scheme, each player has to ask for value from other player by peer-to-peer network for many times, which leads to the low efficiency of the lottery.

Liao et al. [18] propose a lottery system based on blockchain and smart contract. The process of lottery includes four phases, which is initialization, purchasing, closing, verifying. The system uses blockchain to ensure security payments, ticketing and payouts in distribution environments, and guarantees that operations will be property enforced by all interesting entities.

And the Hawk model [19] is used to protect the privacy of the players. However, the winning number is generated by the code of smart contract, players cannot verify the randomness of it. And there is no experiments to test the performance of the proposed scheme.

III. The Preliminaries

A. Blockchain

Blockchain is a decentralized public database based on consensus mechanism, which maintains a growing list of data records, having a linked data structure. Transactions taken place over a period of time are packed into a block by miners. Every block stores the hash pointer of the previous block, so these blocks form a link-list, which is shown in 1.

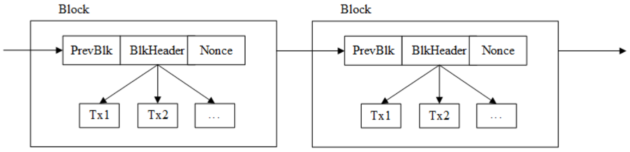

Fig. 1. Structure of blockchain

Blockchain can guarantee the tamperability of data and transactions, which achieved by two schemes. One is decentralized, all the participants have the equal power to view the content of all blocks and get the right to package blocks. The other is consensus mechanism, such as POW, POS and DPOS, which is used to select the bookkeepers and ensures all the network nodes have the same copy of the ledger. As a consequence, data and transactions on the blockchain is hard to be tampered.

B. Smart Contract

The emergence of smart contract makes blockchain not only applicable to the financial fields, but also other fields, such as lottery, electricity transaction and IoT. Smart contract is a piece of code that runs on blockchain. 2 shows the entire process of deploying and executing a smart contract. First, developers program a smart contract and deploy it on the blockchain. Then, the smart contract will create an object that consists of data and functions when a miner packaged it into a block. When outside events trigger the smart contract, the smart contract object will testify the condition of executing, and generates an unverified transaction waiting for miner to verify it and package it into a block. Finally, smart contract accomplish the data modification and funds transfer. It is need to be noticed that the data of smart contract object is allowed to be modified as soon as the condition is satisfied, however, the records of changing data is noted on the blockchain, which is hard to be tampered, as mentioned above.

C. Multi-Party Computation

The main idea of Multi-Party Computation(MPC) is that all the participants work together to compute a function in a special way, and all of them know the output of function, but they do not know the input of others. The Multi-Party Computation used by us is illustrated as follows. Every participant submits a point (x_i,y_i) to a third party, the third party will calculate a polynomial

$$f(x) = a_0 + a_1 * x + a_2 * x^2 + ... + a_n * x^n \tag{1}$$

that goes through all the points submitted by participants. The third party cannot fake in this protocol, because every participant can put their point into the polynomial for testing. And the process of construct and verify a MPC can be depicted by matrix.

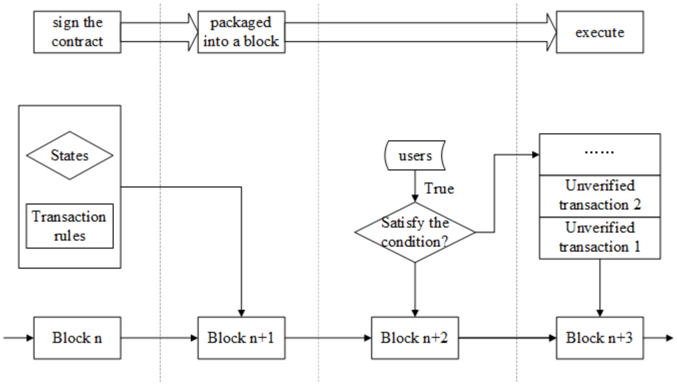

Fig. 2. Process of smart contract

The trusted third party can calculate the matrix equation below to get the coefficient $\{a_0, a_1, a_2, ...a_n\}$ and get the polynomial $f(x)$.

$$\begin{pmatrix} a_0 \\ a_1 \\ ... \\ a_n \end{pmatrix} = \begin{pmatrix} 1 & x_0 & ... & x_0^n \\ 1 & x_1 & ... & x_1^n \\ & & ... & \\ 1 & x_n & ... & x_n^n \end{pmatrix}^{-1} \begin{pmatrix} y_0 \\ y_1 \\ ... \\ y_n \end{pmatrix} \tag{2}$$

Every participant can verify the MPC by verifying the equation below.

$$f(x_i) = y_i \tag{3}$$

IV. Models and Goals

A. System Model

The system model comprises (1) a lottery center, (2) a smart contract that run on the blockchain platform and (3) players that participant in the lottery. The notations of all the parameters in the scheme are summarized in I

The lottery center sets the lottery rules. For simplify, we set a simple lottery rule. Every player selects a number from 0 to 999 as the value of a purchased lottery ticket. If the number is the same as the winning number, the player wins the prize. If more than one player wins the prize, the money will be divided equally and if no one wins the prize, it will be used as the pool for the next round. The smart contract is a piece of code that run on the blockchain platform, the code can be seen by all the people, by which players can buy tickets or verify the fairness of lottery.

TABLE I
SUMMARY OF NOTATIONS

Lottery Center	
LC_{P_k}	Public key of lottery center
LC_{S_k}	Private key of lottery center
$LC_{address}$	Address of lottery center's account on blockchain
$EndTime_{buy}$	The deadline of players submitting commitments of tickets
$EndTime_{open}$	The deadline of players opening lottery commitments
n_w	The winning numbers of the lottery
Players	
i	The unique identification of every player
$PL_{address_i}$	Address of a player's account on blockchain
v_i	The value that bought by a player whose address is $PL_{address_i}$
s_i	The identification code of a player whose address is $PL_{address_i}$
$PL_{P_{k_i}}$	Public key of a player whose address is $PL_{address_i}$
$PL_{S_{k_i}}$	Private key of a player whose address is $PL_{address_i}$
$Hash(.)$	Cryptographic hash function, e.g. SHA-3
Smart Contract	
$SC_{address}$	The address of smart contract on blockchain
$CommitmentList$	Stores all the commitments submitted by players
$TicketList$	Stores all the tickets bought by players
Calculate(.)	A function that calculate the polynomial that contains the winning number
Submit(.)	A function that players submit their commitments
Open(.)	A function that players open their commitments
Verify(.)	A function that players verify the randomness of the winning number

B. Adversarial Model

The adversaries can be lottery center, players, or others who do not participant in the lottery. The adversaries can see all the contents on the blockchain, includes $CommitmentList$ and $TicketList$. And the lottery center can see all the ticket numbers that bought by players. We assume that all the adversaries have the polynomial computing power.

C. System Goals

Our goal is to design a fair and efficient lottery scheme, which can ensure the fairness of lottery result and is public to all the participants.

Goal 1: Random numbers generation.

The winning number is generated randomly, which means that the lottery center cannot intervene the value of winning number and the players cannot predict the value of winning number.

Goal 2: Public verification.

All steps of lottery are public, which means all the people can verify the fairness of the lottery.

Goal 3: Efficiency.

The scheme is efficient, which means the players can buy lottery tickets efficiently and all the people can verify the fairness of lottery rapidly.

V. A Blockchain Based Smart Contract for Fair and Efficient Lottery Scheme

The protocol of the communication between lottery center, players and blockchain is shown in the 3.

A. Deploy

The lottery center deploys a smart contract into blockchain, which is shown in 2. The process can be described as follows:

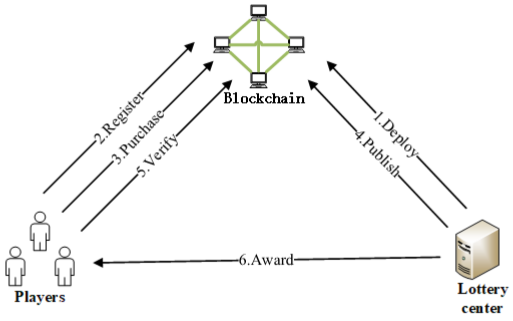

Fig. 3. Lottery transaction steps

1. Lottery center generates two pair of keys, one is (LC_{P_k}, LC_{S_k}), the other is (PL_{P_k}, PL_{S_k}).
2. Lottery center programs the smart contract of lottery by programming language, such as Solidity, C++. The smart contract contains state and transaction rules, such as ticket value of users and specified $EndTime_{buy}$ and $EndTime_{open}$.
3. Lottery center signs the smart contract with its private key LC_{S_k} and sends it to the blockchain. When miners verify the smart contract, it can be packaged to a block successfully, as shown in the 2.
4. Once the smart contract is packaged into a block, it will have an unique address, by which others can execute it. The address of smart contract, $SC_{address}$, is public to all the people, includes players and the lottery center.
5. The lottery center sends its public key $(LC_{P_k}$ to blockchain, which is used to protect the confidentiality of communication.

B. Register

Each player generates his own key pair $(PL_{P_{k_i}}, PL_{S_{k_i}})$, and will receive an address $PL_{address_i}$, which is dispensed by the blockchain platform.

C. Purchase

The process of purchasing a lottery ticket can be described as follows:

1. Every Player chooses his (v_i,s_i), which denotes the ticket value and identification code.
2. Every player sends a commitment $Hash(v_i, s_i)$ to the blockchain by executing the smart contract before $EndTime_{buy}$. As shown in 2, players provide inputs to the smart contract. If the execution condition is met, the smart contract will be triggered and generate a list of unverified transactions. When miners verify the transactions, the list of unverified transactions will be packaged into a new block, which means the smart contract is executed successfully.
3. After the $EndTime_{buy}$, every player has to send his $LC_{P_k}(v_i, s_i)$ to the blockchain by smart contract before $EndTime_{open}$, and the lottery center can get (v_i, s_i) with its private key LC_{S_k}. Then, the lottery center will calculate $Hash(v_i, s_i)$ automatically and see whether it matches the hash value submitted during the previous phase. If the $Hash(v_i, s_i)$ not matches the commitment pre-submitted by player, the ticket can be abandoned.

D. Publish

The process of generating winning number and publishing it to the blockchain can be described as follows:

1. The lottery center treat all each ($Hash(v_i, s_i)$,v_i) that submitted by players as a point (x_i, y_i). And the lottery center trys to get a polynomial $f(x) = s_0 + a_1 * x + a_2 * x^2 + ... + a_n * x^n$ that goes through all the points. The method to get $f(x)$ is Barycentric Lagrange Interpolation, which is an improvement of Lagrange Interpolation. Suppose there are $n + 1$ points $(x_1, y_i), i \in (0, n + 1)$. The center of gravity the weight is defined as:

$$w_j = \frac{1}{\prod_{i=0,i\neq j}^{n}(x_j - x_i)} \tag{4}$$

The Barycentric Lagrange Interpolation is:

$$L(x) = \frac{\sum_{j=0}^{n} \frac{w_j}{x-x_j} y_j}{\sum_{j=0}^{n} \frac{w_J}{x-x_j}} \tag{5}$$

2. The lottery center publish the polynomial to all the participants. Since the coefficient of the polynomial is unpredictable and truly random, so it can be treated as the winning number. Lottery center sends $result = s_0 mod 1000$ to the blockchain by smart contract. The $result$ is the winning number of the lottery.

E. Verify

All the players can verify the randomness of the winning number by validate

$$f(x_i) = y_i \tag{6}$$

If the equation is not true, then the lottery center is guilty of fraud. Players can publish the verification result to the blockchain and the reputation of the lottery center will decline.

F. Award

Winners have to provide his $PL_{address_i}$ and (v_i, s_i) to the lottery center, which can be verified according to the records on the blockchain. If the winners are identified, lottery center can present the award to the winners. Note that this step can be accomplished on the blockchain or offline, which depends on the players' wishes.

VI. Security Analysis

A. Polynomial Construction Attack

If the polynomial $f(x)$ does not exist, which means the lottery has no winning number, This is not allowed in the real lottery. And if there are more than one polynomial $f(x)$ goes through all the ($Hash(v_i, s_i)$,v_i), the lottery center can choose a $result = s_0 mod 1000$ that matches the ticket value of itself or its friends, which break the fairness of lottery.

However, the polynomial $f(x)$ exists and is unique. Suppose there are $n + 1$ players submit ($Hash(v_i, s_i)$,v_i), which is treated as $(x_i, y_i), i \in (0, n + 1)$. Existence and uniqueness of polynomials can be proved as follows.

Suppose that the polynomial that we are going to construct is

$$f(x) = s_0 + a_1 * x + a_2 * x^2 + ... + a_n * x^n \tag{7}$$

The polynomial satisfies the condition:

$$f(x_i) = y_i \tag{8}$$

The following system of linear equations is obtained:

$$\begin{cases} y_0 = s_0 + a_1 * x_0 + a_2 * x_0^2 + ... + a_n * x_0^n \\ y_1 = s_0 + a_1 * x_1 + a_2 * x_1^2 + ... + a_n * x_1^n \\ ...... \\ y_n = s_0 + a_1 * x_n + a_2 * x_n^2 + ... + a_n * x_n^n \end{cases} \tag{9}$$

The determinant of the coefficients of the system is

$$D = \begin{vmatrix} 1 & x_0 & x_0^2 & ... & x_0^n \\ 1 & x_1 & x_1^2 & ... & x_1^n \\ ...... & & & & \\ 1 & x_n & x_n^2 & ... & x_n^n \end{vmatrix} \tag{10}$$

D is a Vandermonde determinant. It can be known from the properties of Vandermonde determinant that when $x_i = x_j (i \neq j)$, $D \neq 0$. So the equation set (1) has a unique solution, which means $f(x)$ and result of lottery is the only certainly.

TABLE II
EXPERIMENTAL CONFIGURATION

Lottery Center Components	Configuration Parameters
CPU	Intel(R) Core(TM) i7-6700U CPU @ 3.40GHz 3.41GHz
Memory	16.00GB DDR
Hard Disk	1TB HDD
OS	Ubuntu 16.0.4
Operating environment of Python	python 3.7.1 Anaconda, Inc
Players	Configuration Parameters
CPU	Intel(R) Core(TM) i5-4200U CPU @ 1.60GHz
Memory	8.00GB DDR
Hard Disk	500GB HDD
OS	Windows 10 Professional

B. Random Numbers Prediction Attack

If the lottery center or players can predict the result of lottery, they can buy the ticket that is bound to win, which means the fairness of lottery is broken.

However, the result of lottery cannot be predicted. Since the players only submit $Hash(v_i, r_i)$ during the purchase phase, and $Hash$ is a one-way function, lottery center knows nothing about v_i and players know nothing about others' v_i. So both of lottery center and players donot know ($Hash(v_i, r_i)$,v_i) of all the players, which means that they cannot calculate $f(x) = s_0 + a_1 * x + a_2 * x^2 + ... + a_n * x^n$ that goes through all the points, and they cannot get $result = s_0 mod 1000$ before $EndTime_{open}$.

C. Bias Attack

The lottery center might try to bias the choice of winning number. In doing so, the lottery center might have different goals each of which violates the fairness of the lottery: for example, it may try to pick a winning number that no user has picked, or it may try to pick a winning number that matches a ticket that a specific user bought.

It does not work either. Since the winning number of lottery comes from the polynomial $f(x) = s_0 + a_1 * x + a_2 * x^2 + ... + a_n * x^n$, all players can check if this polynomial has passed through their own ($Hash(v_i, r_i)$,v_i). So this makes the lottery center cannot fake in the generation of the winning number of lottery.

D. Forging Attack

After the winning number is chosen, a user (and especially the lottery center)may try to forge a winning ticket. We note that the lottery center has an extra advantage since it may know the winning number before it is announced.

But neither the lottery center nor the players can forge a winning ticket without the knowledge of others. Because when you receive the award, you must submit your (v_i, r_i) to blockchain by smart contact. And all the participants can check whether it in the records of ($Hash(v_i, r_i)$,v_i) submitted during Purchasing Phase.

E. Impersonating Attack

Suppose player P_i wins the lottery, but player P_j impersonates P_i to submit (v_i, r_i) to blockchain during the Winning Phase and accept the award that belongs to P_i.

However, anyone cannot pretend to accept an award. Because every time the players execute a smart contract, he or she initiates a transaction on blockchain. Blockchain has a perfect signature mechanism, and every transaction has the initiator's signature, which makes it impossible for others to fake.

VII. PERFORMANCE ANALYSIS

A. Settings

We use Jungle Testnet, a test network for EOS, as our blockchain platform. And a server is used as the server of lottery center. The specific experimental environment is shown in the II.

The length of parameters P_k,v_i,r_i and hash output are listed in the III.

TABLE III
PARAMETERS INFORMATION

Parameters	length(bit)
P_k	1024
v_i	10
r_i	less than 1000
hash output	64

B. Communication Time

The communication time of this mechanism is mainly the interaction time between the players and the blockchain. Players can submit their purchasing requests from the beginning of lottery to $EndTime_{buy}$. We tested the communication cost of purchasing lottery tickets between 1000 and 10000 players.

As shown in 4, the communication costs in our scheme is higner than Grumbach's between 1000 and 4500 players. The reason is that players of BanFEL need to contact with a node of blockchain and wait for the verification of miners, but players of Grumbach's scheme only need to contact with other players and the lottery center. With the number of players increasing, our scheme is less costly in communication than

Grumbach's, because players of Grumbach's scheme need to contact with a large number of other players as the number of players is increasing, but players of BanFEL still only need to contact with a node of blockchain and wait for the verification of miners.

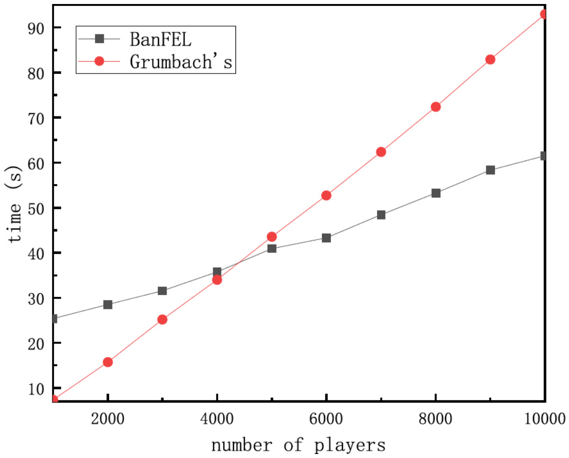

Fig. 4. Communication costs of purchasing lottery numbers

C. *Computation Time*

Obviously, it is difficult for the lottery center to calculate $f(x)$, and the time complexity is $O(n^2+n)$. But lottery centers have high-performance servers and they can outsource the task to other computing platforms. Besides, the real lottery systems do not require lottery centers to disclose winning numbers immediately after the purchases, they always have enough time to compute the winning numbers. Therefore, this will not affect the feasibility of the scheme. However, players have limited computing power, and they want to be able to quickly verify the randomness of winning numbers, that is, whether $f(x)$ goes through the $(Hash(v_i, r_i)$,$v_i)$ of themselves. As shown in 5, we tested the communication costs of verification the randomness of the winning number between 1000 and 10000 players. It is obvious that the computation costs in our scheme is lower than Grumbach's.

VIII. Conclusion

This paper has proposed BanFEL. First, the winning number is generated by the Multi-Party Computation, every player contributes to the generation of the winning number. Second, the process of lottery is public and the result of lottery can be verified by all the participants. The randomness of the lottery result is verifiable, all the players can verify their own contribution to the winning number. The purchase records are published on the blockchain, so the winners of lottery can be verified by all the participants, too. Third, we list several attacks on the lottery system and analyze how to protect against such attacks in our scheme. Last but not the least, We tested the efficiency of the scheme, both the computational time and the communication time were in a relatively low range. Therefore, we consider the mechanism to be efficient.

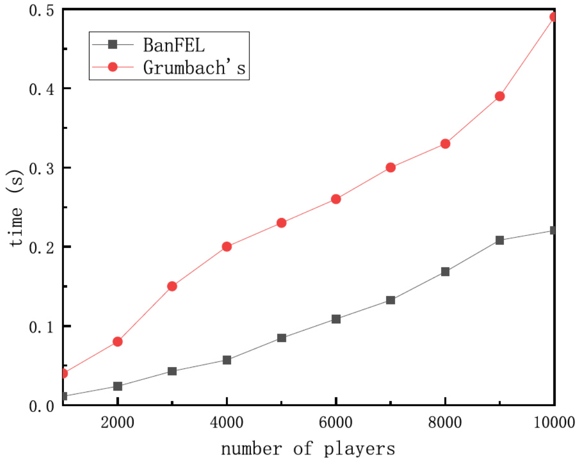

Fig. 5. Verification costs of winning number

References

[1] https://gamblingcompliance.com/premium-content/insights_analysis/global-lottery-growth-eases-fy2017-amid-draw-game-decline-europe.

[2] https://www.desmoinesregister.com/story/news/investigations /2017/06/03/iowa-lottery-rigging-scam-shook-gaming-industry/362328001/

[3] http://baijiahao.baidu.com/s?id=1616730169665425580&wfr=spider&for=pc

[4] Bartoletti, Massimo, Tiziana Cimoli, and Roberto Zunino. "Fun with Bitcoin smart contracts." International Symposium on Leveraging Applications of Formal Methods. Springer, Cham, 2018.

[5] Liao, Da-Yin, and Xuehong Wang. "Applications of Blockchain Technology to Logistics Management in Integrated Casinos and Entertainment." Informatics. Vol. 5. No. 4. Multidisciplinary Digital Publishing Institute, 2018.

[6] Wood, G.: Ethereum: A Secure Decentralised Generalised Transaction Ledger, (2014). http://gavwood.com/paper.pdf

[7] Huh, Seyoung, Sangrae Cho, and Soohyung Kim. "Managing IoT devices using blockchain platform." 2017 19th international conference on advanced communication technology (ICACT). IEEE, 2017.

[8] Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 2016.

[9] Sikorski, Janusz J., Joy Haughton, and Markus Kraft. "Blockchain technology in the chemical industry: Machine-to-machine electricity market." Applied Energy 195 (2017): 234-246.

[10] Christidis, Konstantinos, and Michael Devetsiiotis. "Blockchains and smart contracts for the internet of things." Ieee Access 4 (2016): 2292-2303.

[11] Peters, Gareth W., and Efstathios Panayi. "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money." Banking beyond banks and money. Springer, Cham, 2016. 239-278.

[12] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, (2008). https://bitcoin.org/bitcoin.pdf

[13] Hu, Kexin, and Zhenfeng Zhang. "Fast Lottery-Based Micropayments for Decentralized Currencies." Australasian Conference on Information Security and Privacy. Springer, Cham, 2018.

[14] Miller, Andrew, and Iddo Bentov. ”Zero-collateral lotteries in Bitcoin and Ethereum.” 2017 IEEE European Symposium on Security and Privacy Workshops (EuroSPW). IEEE, 2017.

[15] Pierrot, C., and Wesolowski, B.: Malleability of the blockchain’s entropy. In: ArcticCrypt 2016, pp. 1–20

[16] Lenstra, A.K., and Wesolowski, B.: A random zoo: sloth, unicorn, and trx. NIST Workshop on Elliptic Curve Cryptography Standards 3, 2015.

[17] Grumbach, Stéphane, and Robert Riemann. ”Distributed random process for a large-scale peer-to-peer lottery.” IFIP International Conference on Distributed Applications and Interoperable Systems. Springer, Cham, 2017.

[18] Liao, Da-Yin, and Xuehong Wang. ”Design of a blockchain-based lottery system for smart cities applications.” 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC). IEEE, 2017.

[19] Kosba, Ahmed, et al. ”Hawk: The blockchain model of cryptography and privacy-preserving smart contracts.” 2016 IEEE symposium on security and privacy (SP). IEEE, 2016.