# Fairness Protection Method of Vickery Auction Based on Smart Contract

Yuan Yu, Li Yang(✉), Wenjing Qin, and Yasheng Zhou

Xidian University, Xi'an 710071, Shaanxi, China
yangli@xidian.edu.cn

**Abstract.** In the Vickery auction rules, the highest bidder gets the goods, but deals with the second highest bid. Although Vickery auction rules can solve the problem of information asymmetry between buyers and sellers, the common fairness problems outside the bidding rules, such as buyer collusion, multi-price bidding and seller price raising, still cannot be solved. This paper proposes a new fairness protection method of Vickery auction. It builds an auction platform based on blockchain, and realizes fair bidding to prevent collusion and ensure the only bid through the automatic execution mechanism of smart contract. At the same time, this method protects bidding privacy and excludes the seller's bid based on secure multi-party computation. It improves the security of Vickery auction in practical application. This paper also builds a fairness evaluation model of bidding mechanism, and proves that the method has good performance in protecting bidding fairness.

**Keywords:** Vickery auction · Blockchain · Smart contract · Secure multi-party computation · Evaluation model

## 1 Introduction

Auction is a kind of spot trading mode in which the auction house specialized in auction business accepts the entrustment of the owner, displays the goods to be auctioned to the buyer at the specified time and place according to certain regulations and rules, so as to maximize the interests [1]. In the auction, the information asymmetry between the seller and the buyer often leads to the loss of fairness. For example, the British auction follows the principle of the one with the highest price. If the buyer collude to bid, the final price can be reduced and the fairness to the seller will be damaged.

In order to solve the problem of information asymmetry, Professor William Vickery, the Nobel Laureate in economics, proposed Vickery auction [2]. The rule of Vickery auction is: in the auction, the buyer with the highest bid is

We would like to thank the anonymous reviewers for their careful reading and useful comments. This work is supported by the National Natural Science Foundation of China (Program No. 62072352, 62072359).


W. Shi et al. (Eds.): SPNCE 2021, LNICST 423, pp. 15–34, 2022.
https://doi.org/10.1007/978-3-030-96791-8_2

qualified to buy goods, but he only needs to pay the second highest price. Vickery auction ensure the optimal Pareto efficiency, that is, after reducing the influence of the winning bidder on the final price, the buyer can eliminate the premium or decision-making error caused by guessing game to the other buyers when bidding, so as to produce a bid as close to the real value of the goods as possible, and eliminate the fairness loss caused by information asymmetry.

Vickery auction, as a representative form of sealed auction, can well solve the problem of information asymmetry in auction, and help to improve the fairness of other sealed auction. However, there are still many fairness problems caused by operation outside the mechanism. The fairness of auction will be affected by the decrease of final price caused by the collusive bidding of the buyer. As the case proposed by Athey et al. [3], in the infinitely repeated Bertrand game, collusive bidding can reduce costs for firms. The manipulation of the auction result caused by the buyer's multiple bidding prices will damage the fairness of auction. As the case proposed by Axel et al. [4], multiple bidding happens in second price Internet auctions with a fixed end time, such as those on eBay. The participation of the seller in the auction will lead to higher final price. If the seller knows the highest price and the second highest price in advance, he can bid between the two, so that the buyer has to deal at the higher price offered by seller on purpose. Therefore, a privacy protection scheme [5,6] for bidding price is very necessary.

To eliminate the privacy and security problems caused by the illegal operation of buyers and sellers in Vickery auction. From the perspective of the seller, an effective method should be proposed to prevent the buyer from colluding in bidding, so that the buyer can only bid honestly once. From the buyer's point of view, we should put forward effective method to avoid the seller's price raising, especially in shielding the buyer's bid and excluding the seller's operation. How to find an effective method to meet the above needs has become the main goal of the method proposed in this paper.

In order to solve the above problems, this paper uses blockchain, smart contract and secure multi-party computation to implement a fairness protection method of Vickery auction. The auction platform for seller and buyer to trade is built on the blockchain, and the auction process is automatically executed through the smart contract to protect the buyer's bidding privacy and ensure that the buyer has only one bid. Secure multi-party computation is used to ensure the privacy of the buyer's bid and exclude the seller's bid, which provides a fair solution for the practical application of Vickery auction. The main contributions include:

- A fairness protection method of Vickery auction based on smart contract is proposed, which realizes fair Vickery auction through invisible buyer's only bid collection and non-interference final price privacy calculation.
- A fairness evaluation model of bidding mechanism is constructed to verify the good fairness performance of our method and enrich the research perspective of bidding evaluation model.

– The fairness of our method is at least 2.5 times better than that of SAP scheme and ASAS scheme in both mean standard deviation method and Delphi method.

## 2 Related Work

The security of Vickery auction can be enhanced by adding privacy computing method based on cryptography. For example, in 2003, Suzuki et al. [7] used homomorphic encryption technology to strengthen the privacy security of the Vickery auction mechanism of combinatorial auctions. However, due to the addition of random mask value, the scheme will reveal some other information besides the auction results.

In 2008, Sekhavat et al. [8] proposed ASAS anonymous secure auction scheme, which has better performance than EOBA and SAP schemes. However, all participants (certification authority, seller, auctioneer, payment gateway and multiple buyers) need to hold public and private keys and certificate to verify their identities, and the communication in the bidding execution process is still complex.

In recent years, related work mainly focuses on the rational allocation of resources by using the Vickery auction principle. For example, Al-manthari et al. [9] solved the congestion pricing problem of wireless networks using the Vickery auction principle in 2011, and Zhang et al. [10] used the Vickery auction principle to select the auxiliary relay in satellite ground sensor networks in 2019. Not only in the Internet related industries, Vickery auction is also applied to the auction of animal husbandry resources [11]. When people need to choose the right supplier in the supply chain [12], Vickery auction also helps a lot. But little has been done to focus on ensuring fairness while enhancing the privacy of Vickery's auction.

To address the fairness and privacy issues of vickery auctions, and the need for invisible and anonymous buyers, unique bids, and non-interference by sellers, as a distributed shared database technology, blockchain technology has the characteristics of decentralization, transparency, fairness and openness, which coincides with the requirements of Vickery's auction.

Blockchain is widely used in different fields such as data outsourcing [13], recommendation system [14], edge computing [15] and so on because of its anonymity, de trust, point-to-point, traceability and non tamperability. At present, the idea of building an auction platform based on blockchain and smart contract has been relatively mature. For example, a transactive energy auction that operates without the need for a trusted entitys oversight is proposed by Hahn et al. [16]. However, this method does not consider the impact of the seller's operation on the fairness in the auction. Wang et al. proposed a decentralized electricity transaction mode for microgrids based on blockchain and continuous double auction (CDA) mechanism [17]. Galal et al. present a smart contract for a verifiable sealed-bid auction on the Ethereum blockchain [18]. However, they need a credible auction notary to verify the seller and the buyer's commitment, and those who participate in the auction will not get the return value of the failure bid. In reference [19], Sanchez et al. Proposed a blockchain based auction

system Raziel, which combines secure multi-party computing and zero knowledge proof. The system ensures the privacy, correctness and verifiability of Auction Contracts running on the blockchain. However, because secure multi-party computing and zero knowledge proof are used to realize the complete anonymity of identity, the overall scheme is complex and difficult to popularize. At present, the challenge of Vickery auction fair protection method based on smart contract is that there is no standardization of fairness, that is, there is no quantitative method to evaluate fairness, so it is difficult to find the entry point to maintain fairness and to quantitatively evaluate the scheme.

After years of development, Vickery auction has integrated many scenes and fields, but how to improve the fairness of the operation outside the mechanism under the premise of ensuring privacy security, and how to use reasonable evaluation criteria to measure the effect of the auction mechanism still need more exploration.

In order to put forward a better fairness evaluation model of auction mechanism, we studies many evaluation mechanisms. Hobbs et al. describe a Vickrey-Clarke-Groves auction for supply and demand bidding in the face of market power and nonconcave benefits [20], which focus on its risks being revenue deficient, can be gamed by cooperating suppliers and consumers, and is subject to the information revelation and bid-taker cheating. Chen et al. focuses on mechanism design for quality assignment combinatorial procurement auctions [21]. their model focuses on how the participants maximize social surplus, the difference between gross utility and total cost in electronic procurement. The evaluation model proposed in this paper focuses more on fairness performance, and constructs a linear objective function by combining privacy evaluation and revenue evaluation.

## 3 Fairness Protection Method of Vickery Auction

This section introduces the fairness protection method of Vickery auction based on smart contract. The method consists of two stages: invisible buyer's only bid collection and non-interference final price privacy calculation. The fairness protection method of Vickery auction diagram is as Fig. 1.

### 3.1 Method

The two stages can be divided into four steps with temporal relationship, which together form the process of realizing Vickery auction. For each step, use arrows to show the data transfer relationship between them, build bidding platform on the blockchain, deploy smart contracts on the console, and return the transaction results every time the contracts are executed to collect bids. The auction parameters formed in the smart contract are automatically set into the privacy computation framework and translated into circuit files through the circuit compiler. Finally, the privacy calculation results are returned to the seller and the buyer.

The data transfer relationship also exists between the seller, the buyer and the auction platform. The seller and the buyer nodes need to submit identity authentication to join the blockchain. The blockchain network reaches a consensus on synchronization messages to the seller and the buyer nodes. Every time the buyer submits a bid by calling the smart contract, he will get the result of whether his bid is successful or not, and if it fails, the buyer can prepare for the next step in advance.

In the bidding process, the invisible buyer's only bid collection restricts the buyer's fair operation, and the non-interference transaction price privacy calculation restricts the seller's fair operation. To achieve the fairness of Vickery auction, both restrains should be met.

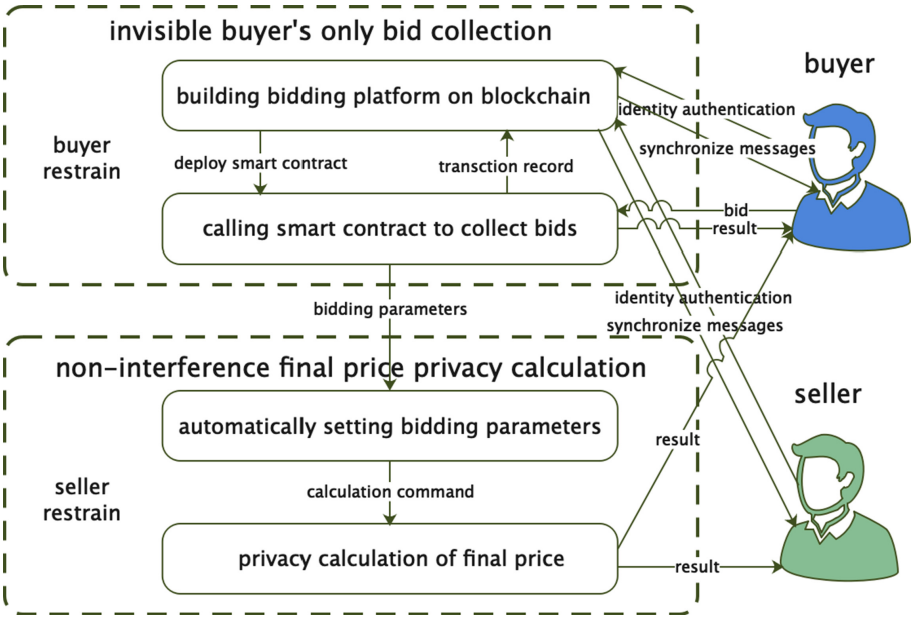


**Fig. 1.** Fairness protection method of Vickery auction.

### 3.2 Definition

In the process of online auction, in order to prevent the buyer from bidding collusion to reduce the final price and damage the fairness of the seller, it is necessary to make the buyer invisible. On the other hand, the invisibility of the bid also guarantees the fairness of the buyer and shields the seller to prevent the seller from manipulating. The following gives the basic definitions of invisible of buyer, only bid and non-interference of seller as the focus of the method proposed in this paper. The restrains of the seller and the buyer will be formalized to facilitate the quantification of the subsequent evaluation model.

**Definition 1 (invisible of buyer).** *For the buyer* $BD_1$, $BD_2$ ,..., $BD_n$ *of* n *bids in the bidding process, the bid* $P_i$ *of any buyer* $BD_i$ *is known only by himself,* i ∈ *1, 2, ..., n. Because the buyer is anonymous, he can not ask other buyers for final price by means of communication, and the seller* SE *has no right to view any* $P_i$*, so other buyers can not obtain* $P_i$ *by asking the seller* SE*, then the bidding process is said to be invisible to the buyer.*

According to *Definition* 1, the invisible bidding process of the buyer can avoid the buyers' collusion because they can't see other's bid. Invisible principle also benefits the buyer, shielding the seller from participating in the auction. But if we want to eliminate the manipulation of the bidding process caused by the buyer's multi-price bidding, we need to meet the formal definition of the only bid.

**Definition 2 (only bid).** *For the buyer* $BD_1$, $BD_2$, ..., $BD_n$ *of* n *bids in the bidding process, any buyer* $BD_i$ *can only have one final bid* $P_i$, i ∈ 1, 2, ..., n. *If the buyer* $BD_i$ *needs to change the bid* $P_{i0}$ *to* $P_i$*, it needs to replace the original bid through the mapping mechanism* $M \rightarrow M_0{:}\{\{BD_i \rightarrow P_{i0}\} \rightarrow \{BD_i \rightarrow P_i\}\}$*, then the bidding process satisfies the only bid principle.*

According to *Definition* 2, it can be seen that the only bid principle can avoid the buyer manipulating the final price through multi-price bidding, and realize the fairness of the auction. *Definition* 1 and *Definition* 2 restrict the operation for the buyer's fairness, and the formal *Definition* 3 gives the definition of non-interference as the restrain on the seller's operation.

**Definition 3 (non-interference of seller).** *When calculating the bidding result* R*, calculation system should follow the rule of* C: R = bidding ($pc_1$ (P) → BD, $pc_2$ (P))*, in which* $pc_1$ *gets the highest bid through privacy calculation,* $pc_2$ *gets the second highest bid through privacy calculation. For the buyer* $BD_1$, $BD_2$, ..., $BD_n$ *of* n *bids in the bidding process and their bid* $P_i$, i ∈ 1, 2, ..., n. *The seller* SE *can neither obtain nor modify, and the seller* SE *cannot bid, the final price calculation process is said to satisfy the non-interference of seller principle.*

According to *Definition* 3, non-interference of seller principle can avoid the seller's participation in bidding, eliminate the hidden danger of the seller's price raising, and ensure the fairness of the buyer's bidding.

## 4 Invisible Buyer's Only Bid Collection

This section introduces the first stage of fairness protection method of Vickery auction based on smart contract - invisible buyer's only bid collection. Section 4.1 gives the model and architecture of building an auction platform on blockchain, and Sect. 4.2 gives the algorithm of calling smart contract to collect bids.

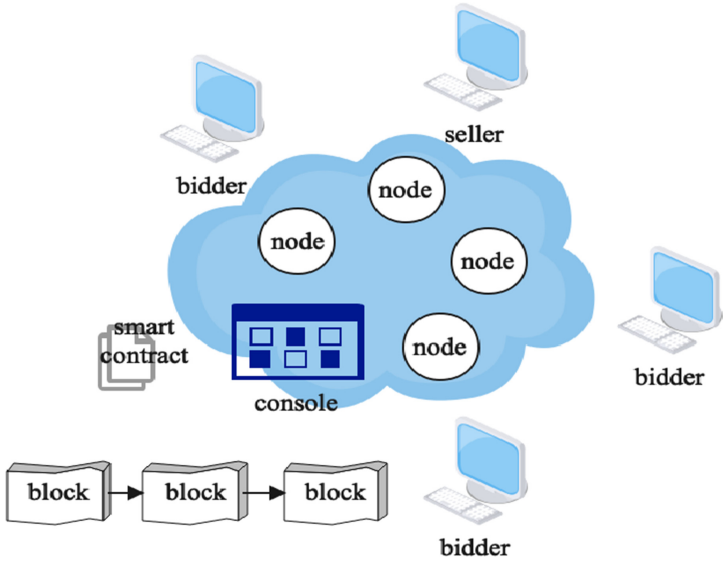


**Fig. 2.** Network node communication model.

### 4.1 Building Auction Platform on Blockchain

The blockchain auction platform is the basis for the buyer and seller to conduct node communication, data transmission, on-chain interaction and information synchronization. It can remove the dependence of bidding activities on the trusted third party, and transfer the trust of institutions to the trust of rules. The construction of blockchain auction platform can realize the network node communication model as Fig. 2.

The seller and the buyer exist in the blockchain network as indistinguishable nodes. They interact with the blockchain through the console to complete the functions of deploying contracts and querying data on blockchain. They are interconnected to form a blockchain network, jointly maintain a consensus information blockchain that follows the timing rules [22], seize the blocks according to the consensus way on blockchain, and verify and retrieve the information synchronization. As for the size of data to be stored locally, users can set their own storage policies.

The experimental platform of this paper is built by FISCO BCOS. It is an enterprise level financial permissioned blockchain platform, which was independently developed by the open source working group of Financial Blockchain Shenzhen Consortium in 2017. Because FISCO BCOS meets the national security standard, the environment and configuration are relatively lightweight, and has good scalability, this paper will use it as the technical basis for building a blockchain. Detailed technical documentation and enthusiastic community maintainers are also the reasons why we chose it. This paper focuses on the fairness

construction of the method, and does not discuss the security of the platform too much.

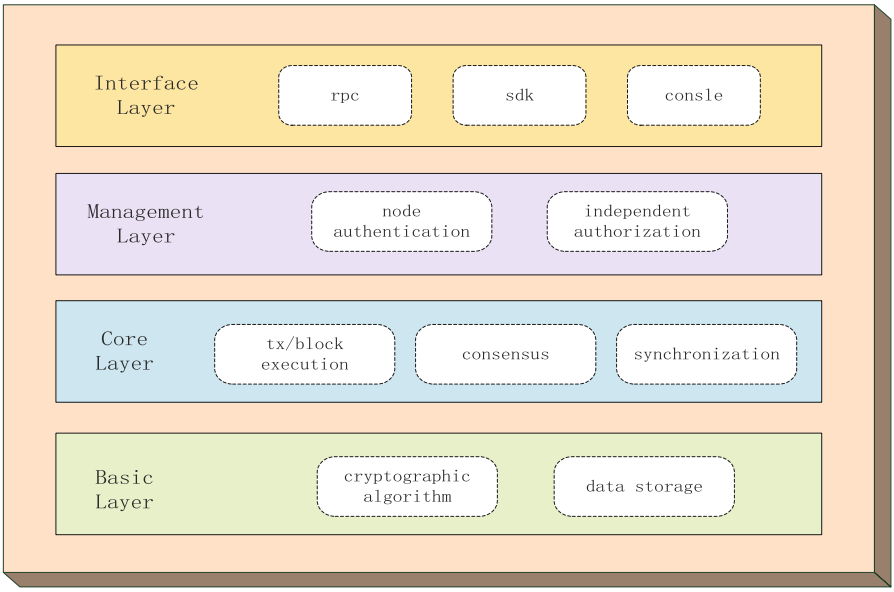


**Fig. 3.** Architecture of the blockchain auction platform.

Figure 3 shows the architecture of the blockchain auction platform. The blockchain auction platform is composed of interface layer, management layer, core layer and basic layer. The interface layer is responsible for controlling external access, the management layer does node authentication and independent authorization, the core layer completes the transaction and block execution and carries out consensus identity synchronization. The basic layer provides cryptographic algorithm library and local data storage.

### 4.2 Calling Smart Contract to Collect Bids

The key of fairness protection of Vickery auction based on smart contract is whether the mechanism of collecting buyer's bid can achieve fairness. Using the characteristics of automatic execution and non-interference of smart contract, an invisible buyer's only bid collection auction algorithm is designed as *Algorithm* 1.

According to *Algorithm* 1, the smart contract will judge the calling address. If the contract owner (i.e. the seller) offers bid, the bid will be returned to realize the fairness of excluding the seller to raise the price.

The highest price is *highest*, and the second highest bid is *secondHighest*. The buyer who bids above the *highest* gets the right to buy temporarily. *Highest* and

**Algorithm 1.** Smart Contract for Vickery Auction

```
Input: address, price
Output: result
initialize highest, secondHighest;
if now <= start + time then
    if address = contractOwner then
        send(price, address);
        return result;
    end
    if price > secondHighest then
        if price > highest then
            if address = bidder then
                highest = price;
            else
                secondHighest = highest;
                highest = price;
                bidder = address;
                send(highest, bidder);
            end
        else
            secondHighest = price;
            send(price, address);
        end
    end
end
if now > start + time then
    send(secondHighest, contractOwner);
    send(highest − secondHighest, bidder);
end
return result;
```

*secondHighest* make corresponding changes. When the bid is above the *secondHighest* but does not exceed the *highest*, only the *secondHighest* is updated. After the bidding, the *secondHighest* is sent to the contract owner (i.e. the seller), and the remaining price difference between *highest* and *secondHighest* is returned to the buyer.

At the same time, *Algorithm* 1 can ensure the only bid. When the buyer's bid is higher than the *highest* he has given, it replaces the *highest* instead of reducing the *highest* to *secondHighest*; when the buyer's bid is between the *highest* and the *secondHighest* he has given, it replaces the *secondHighest*.

Three bidding prices are always stored in the smart contract, and the results of Vickery auction are adjusted according to the size relationship between them. *Algorithm* 1 satisfies both the buyer's invisibility and the only bid. From *Definition* 1 and *Definition* 2, we can see that it satisfies the restrains on the fair operation of the buyer.

## 5 Non-interference Final Price Privacy Calculation

This section introduces the second stage of fairness protection method of Vickery auction based on smart contract, which is non-interference final price privacy calculation, including automatic setting of bidding parameters and privacy calculation of final price.

After the auction smart contract expires, the script will automatically set the bidding parameters to the privacy computation framework, write the circuit program in the docker container, run the multi-party computation framework, and generate the circuit file according to the program.

Firstly, we introduce the millionaires problem in two-party secure computing [23] as the basis of this paper's multi-party privacy computation. To calculate who is richer between the two millionaires without disclosing their specific property, suppose that the secret inputs of Alice and Bob are $I_a$ and $I_b$ respectively, the process is as follows:

- Bob generates an $n$-bit random integer $x$, encrypts it with Alice's public key to get $EnA(x)$, and sends $EnA(x) - I_b + 1$ to Alice.
- Alice calculates every $y_u = DA(k - I_b + u)$, where $u = 1, 2, \ldots, n$, to generate $n/2$-bit random prime $p$, and calculates $z_u = y_u \bmod p$.
- Each calculated $z_u$ is used to compare with $I_a$. If $z_u$ is larger, $z_u + 1$ is sent. Bob can judge the size relationship between $I_a$ and $I_b$ by whether it is equal to $x \bmod p$.

Process of two-party secure computing is shown in sequence diagram as Fig. 4. In addition to the data transfer between Alice and Bob, every interaction between Alice or Bob and himself is a calculation or encryption and decryption operation to change the data.

This two-party secure computing scheme is extended to three parties, which can be used as the final price privacy computing principle in this paper. Because the current highest bid and the second highest bid need to be saved in the smart contract and compared with the new bid generated by calling the contract, only three parties need to compare the size.

Process of three-party secure computing is shown in sequence diagram as Fig. 5. Suppose that the highest bid stored in the contract is Alice's bid $I_a$, the second highest bid is Bob's bid $I_b$, and the current bid generated by Charlie calling the contract is $I_c$. The calculation process is as follows:

- Charlie generates an $n$-bit random integer $x$, encrypts $En(x)$ with the public key of Alice and Bob, and sends $En(x) - I_c + 1$ to Alice and Bob.
- Alice and Bob compute every $y_u = D(k - I_c + u)$ and $h_u = D(k - I_c + u)$, where $u = 1, 2, \ldots, n$, to generate $n/2$-bit random prime $p_1$ and $p_2$, and calculate $z_u = y_u \bmod p_1$ and $l_u = h_u \bmod p_2$.
- The calculated $z_u$ and $l_u$ are used to compare with $I_a$ and $I_b$. If $z_u$ is larger, $z_u + 1$ will be sent. If $l_u$ is larger, $l_u + 1$ will be sent. The size relationship of three bids can be determined respectively.

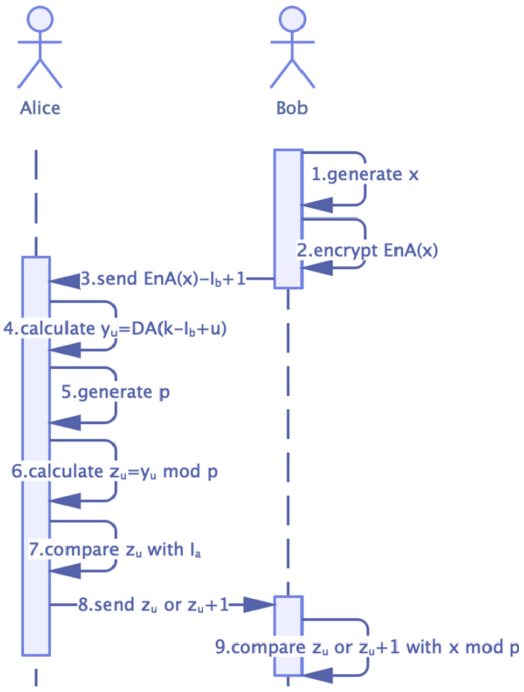


**Fig. 4.** Two-party secure computing.

We can get the three-party privacy calculation principle of the final price, which satisfies the non-interference of the seller. From *Definition* 3, we can see that it satisfies the restrain on the fair operation of the seller. Combined with the three-party comparison mechanism in *Algorithm* 1, the newly proposed bid only needs to compare with the current highest price and the current second highest price. Therefore, it is most appropriate to use it as Charlie in the three-party secure computation, using the common public key encryption of Alice and Bob, and comparing with the other two parties after calculations.

## 6 Fairness Evaluation Model of Bidding Mechanism

Bidding mechanism is a kind of market mechanism that determines the allocation of resources through a series of clear rules and the price determined by the buyer's bidding [24]. That is to say, in a certain time and place, through a certain organization, the specific goods or property rights are transferred to the highest bidder in the form of public bidding.

In the study of the evaluation index of auction mechanism, it is the cornerstone of the establishment of evaluation to formulate the measurement standard according to the actual demand. Considering the shortcomings of the related work listed in Sect. 2, this paper chooses privacy protection and bidding income

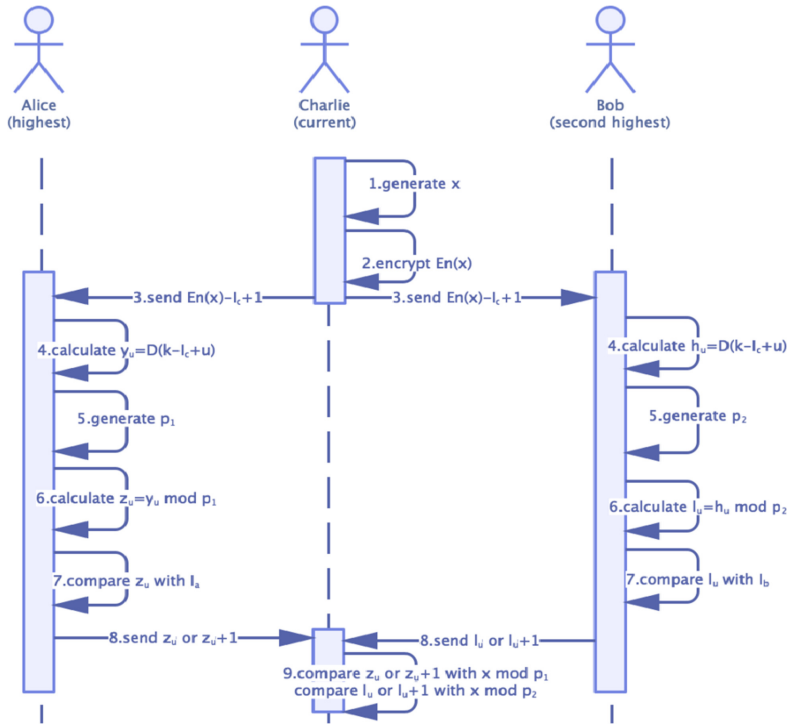


**Fig. 5.** Three-party secure computing.

as the evaluation content of the objective function to solve the problem of the seller and buyer's operation violation.

In the definition of fairness restrains, both invisible and non-interference need to be quantified by privacy protection in evaluation mechanism. Similar evaluation ideas are used to improve the efficiency and utility of mobile crowdsourcing systems [25] and the only bid is realized by algorithm in smart contract. In economics, revenue maximization [26] is an important index to evaluate the bidding mechanism, so the bidding income is also listed as the content of the evaluation mechanism proposed in this paper.

This section formulates the quantitative fairness evaluation model of bidding mechanism, and selects the relevant bidding mechanism to evaluate and compare with the similar method. The objective function $F_A$ of fairness evaluation of bidding mechanism is as follows:

$$F_A = \alpha P_n + \beta B_n \tag{1}$$

$P_n$ is the evaluation of privacy protection, which is positively related to the fairness evaluation, $B_n$ is the evaluation of bidding income, which pursues the principle of profit maximization by bidding mechanism, $B_n$ is positively related to the fairness evaluation, and $\alpha$ and $\beta$ are the weight parameters.

$F_A$ is a linear programming model, because our main goal is to select the optimal method through the quantitative calculation of the objective function. When designing the evaluation mechanism, there is often a need to transform the multi-objective programming model into the single objective programming model [27], so the linear weighted method of objective function has become the mainstream evaluation model.

For the design of evaluation mechanism in this paper, defining the proportional or inverse relationship between each part of the evaluation content and the objective function, and how to properly set the weight parameters are the key problems to be solved.

Section 6.1 gives three mechanism assumptions including consistency assumption, distribution assumption and honesty assumption. Section 6.2 introduces privacy protection evaluation $P_n$ and Sect. 6.3 introduces bidding income evaluation $B_n$.

### 6.1 Mechanism Assumption

- Consistency assumption: the fairness evaluation of bidding mechanism has nothing to do with buyer seller node parameters and network environment. The communication ability and computing ability of the node are regarded as the same.
- Distribution assumption: buyer bids are independent of each other and subject to uniform distribution $D$ on [0, $M$], where $M$ is the highest bid. This assumption is abstracted from the law of bidding price in practice, which presents a monotonic increasing law.
- Honesty Assumption: buyer offers bid $v$ honestly. In order to eliminate the behavior deviation of bidders affected by game theory, the buyer is supposed to bid honestly on the premise that the bid is invisible.

The consistency assumption aligns the node environment, the distributed assumption abstracts the bidding into a mathematical model, and the honesty assumption eliminates the error.

### 6.2 Privacy Protection Evaluation

When researching the evaluation index of privacy protection, the effect of privacy protection is measured by the similarity of privacy data distribution [28]. Privacy protection evaluation $P_n$ is calculated based on string similarity in transaction execution results after one-way function processing of buyer offer data:

$$P_n = \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} Sim(s_i, s_j) - n}{2nd} \tag{2}$$

where $d$ is the distance between similarity intervals. Privacy data should ensure that the distribution similarity among data is as average as possible to achieve the purpose of being difficult to distinguish. The string $s_1$, $s_2$ similarity formula is as follows:

$$Sim(s_1, s_2) = \frac{\sum_{i=1}^{len} u(i)}{len} \tag{3}$$

where len is the larger length of string $s_1$, $s_2$, and the formula is as follows:

$$len = max(length(s_1), length(s_2)) \tag{4}$$

For different strings $s_1$, $s_2$, the position valid value *u(i)* is expressed as:

$$u(i) = \begin{cases} 1, & s_1(i) = s_2(i) \\ 0, & other \end{cases} \tag{5}$$

where *i = 1, ..., len*. If the characters in the corresponding positions are equal, *u(i)* value of 1, unequal or exceed the string length, *u(i)* value of 0.

Through the calculation of privacy protection evaluation $P_n$, we can quantify *Definition* 1 and *Definition* 3, and introduce fairness based on privacy security into the evaluation model of bidding mechanism.

### 6.3 Bidding Income Evaluation

When researching the evaluation index of bidding profit, the profit maximization effect is measured by the incentive compatible mechanism DSIC under the dominant strategy. Referring to the Bayesian model in DSIC mechanism [29], the expected revenue of the auction is designed to be calculated based on *(x, p)* expected $E$ which satisfies the DSIC nature as follows:

$$B_n = \frac{nw}{\sum_{i=1}^{n} v_i E_i} \tag{6}$$

where $w$ stands for final price, $v_i$ stands for buyer's honest bid, and every expect $E_i$ to be calculated as follows:

$$E = \int_0^M x f(x) dx \tag{7}$$

where $M$ is the highest bidding price, $f$ is the density function of distribution $D$, $x$ is the buyer's bid. As (6), the income of the bidding mechanism is inversely proportional to the average value of the product of the buyer's honest bid and the best profit expectation, and is directly proportional to the final price. Because the closer the final price is to the average value, the farther away it is from the optimal value.

In the bidding, the buyer may raise his own offer in reference to another person's bid, resulting in an increase in the final price, or the seller may lower the final price without knowing the true offer $v$ in the buyer's mind. Introducing virtual bid $\varphi_i$ to measure fluctuations in final price caused by information as follows [24]:

$$\varphi_i(v_i) = v_i - \frac{1 - D(v_i)}{f(v_i)} \tag{8}$$

Through the calculation of $B_n$, this paper introduces fairness based on maximum profit for the evaluation model of bidding mechanism. According to the fairness method in this paper, it can eliminate the premium and price depression in the process of bidding, which is closer to the real price distribution.

As (1), we combine Sect. 6.2 and Sect. 6.3 to set appropriate weight parameters $\alpha$ and $\beta$. The evaluation mechanism proposed in this paper can comprehensively show the privacy performance and revenue performance, and can objectively describe the fairness of bidding mechanism. Detailed evaluation and comparison with other similar methods are shown in Sect. 7.

## 7 Experimental Result

According to the method and model introduced in this paper, Vickery auction based on smart contract is constructed as follows: A four node permissioned blockchain is built on the Ubuntu 16.04 system as a data communication platform for bidding. One of the nodes is used as the seller to write the bidding smart contract in *Solidity* language and deploy it to the console through *solc* compilation. The other three nodes call the contract to bid as the buyer, and the automatic execution script is written in *Linux Shell*. The secure multi-party computation framework uses *Wysteria* in docker container to convert the circuit program of three party comparison into the corresponding garbled circuit file [30].

This experiment realizes the fairness protection method of Vickery auction based on smart contract. Now we use the fairness evaluation model proposed in *Sect.* 4 to calculate the $F_A$ of this method and the comparison method SAP and ASAS.

### 7.1 Data Set

Different buyer node calls the smart contract to bid on the console for five times. After each successful call of the smart contract, the corresponding transaction hash is generated, and the transaction hash field is manually extracted from the transaction return result. ASAS scheme uses RSA as public key encryption.

In order to fully consider the possible situations in the practical application, the experiment also produces failed smart contract calls. We find that when the smart contract fails to be called, the console will directly output a failure prompt without generating transaction information.

The bidding data of the buyer obeys the uniform distribution and satisfies the monotonic increasing property. Every two groups of different successful transaction hash data fields use *matlab* to calculate the string similarity, which is expressed as a matrix:

$$\begin{bmatrix} 1.0000 & 0.0156 & 0.0156 & 0.0154 & 0.0149 \\ 0.0156 & 1.0000 & 0.0159 & 0.0161 & 0.0164 \\ 0.0156 & 0.0159 & 1.0000 & 0.0167 & 0.0159 \\ 0.0154 & 0.0161 & 0.0167 & 1.0000 & 0.0163 \\ 0.0149 & 0.0164 & 0.0159 & 0.0163 & 1.0000 \end{bmatrix}$$

The results show that the model has a small range of privacy between [0.0149, 0.0167], which maintains at a stable level. The model has good privacy performance. Calculate $P_n$ according to the similarity is 8.8222.

It is easy for us to explain some properties of matrix. The reason why the diagonal element value is unified as 1.0000 is that the distribution similarity of itself is exactly the same. Diagonal symmetric elements are equal because two identical elements get the same result no matter they are in the same calculation order.

According to the experimental data, the highest bid is 4, the final price is 3, and the buyer's bid satisfies the uniform distribution of [0, 4]. From this, for a sealed-bid auction like the Vickery auction, $B_n = 3.7500$ is calculated.

We suppose that the British auction, which is a public auction, has the same consistency assumption as Vickery auction. According to (6), $B_n = 5.0000$ is calculated. However, this method has no means of privacy protection, $P_n = 0.0000$.

### 7.2 Experimental Results

Calculate the privacy protection evaluation $P_n$ and bidding income evaluation $B_n$ of this method, SAP scheme [31] and ASAS scheme. In order to increase the richness of the experiment, we also calculate the public auction that follows the higher price. This kind of auction is also called British auction [32]. All experimental results are shown in Table 1.

The bid of SAP scheme is visible to the trusted third party, so the data similarity is 0.0000. Although the data similarity performance for ASAS is better than the method in this paper, it has a large range of variation between [0.0116, 0.0581], and the comprehensive privacy performance is poor.

Every two groups of different successful RSA encryption results data fields use *matlab* to calculate the string similarity, which is expressed as a matrix:

$$\begin{bmatrix} 1.0000 & 0.0581 & 0.0406 & 0.0116 & 0.0291 \\ 0.0581 & 1.0000 & 0.0174 & 0.0174 & 0.0174 \\ 0.0406 & 0.0174 & 1.0000 & 0.0465 & 0.0233 \\ 0.0116 & 0.0174 & 0.0465 & 1.0000 & 0.0291 \\ 0.0291 & 0.0174 & 0.0233 & 0.0291 & 1.0000 \end{bmatrix}$$

**Table 1.** Experimental results

| Method | $P_n$ | $B_n$ |
|---|---|---|
| This paper | **8.8222** | **3.7500** |
| SAP | **0.0000** | **3.7500** |
| ASAS | **0.6250** | **3.7500** |
| British auction | **0.0000** | **5.0000** |

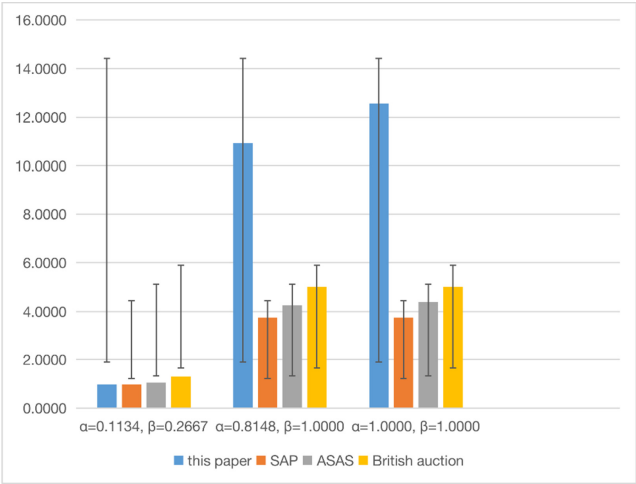


**Fig. 6.** Comparison of fairness evaluation of bidding methods.

Although the value of $\alpha$ and $\beta$ can be set and adjusted subjectively by the users of the evaluation model according to the degree of attention to privacy protection and bidding income, this paper still chooses the parameters to provide general models based on several standardization and factor analysis methods to calculate $F_A$.

Referring to the standard deviation method [33], the value of variables is adjusted to [0, 1] interval, so that privacy protection and bidding income can play an equal role. The resulting $\alpha = 0.1134$ and $\beta = 0.2667$. However, the main purpose of this standardization method is to reduce the variable gap. Compared with the value of $F_A$, the parameter gap between different models should be compared.

Referring to the mean standard deviation method [34], adjust the variables evenly to the interval. The resulting $\alpha = 0.8148$ and $\beta = 1.0000$. Compared with the standard deviation method, this mean standard deviation method partially protects the scaling proportion.

Referring to the Delphi method [35], set unbalanced parameters in subjective simulation expert scoring and calculate $\alpha = 1.0000$ and $\beta = 1.0000$. The evaluation result of the three methods is as Fig. 6.

By adjusting the values of $\alpha$ and $\beta$, we can balance the model's emphasis on privacy protection and bidding income. Experimental results show that the proposed method has similar fairness performance with SAP scheme and ASAS scheme in standard deviation method. But in mean standard deviation method and Delphi method, the fairness performance of our method is improved by 2.9–5.7 times for SAP scheme and 2.6–4.3 times for ASAS scheme.

For the British auction, the public auction method, the best interests of the seller are better protected, but compared with the Vickery auction, the privacy

protection has some shortcomings. Therefore, from the experimental results, we can see that the British auction performs slightly better than the general Vickery auction method, but compared with the method proposed in this paper, the performance of privacy protection is slightly worse.

## 8 Conclusion

Based on the smart contract, the fairness protection method of Vickery auction is realized, and the invisible of buyer, the only bid and the non-interference of seller are defined. The fairness restrains between the buyer and the seller is realized through the invisible buyer's only bid collection and the non-interference final price privacy calculation. In the stage of invisible buyer's only bid, the auction blockchain platform is built, and the smart contract is deployed. In the non-interference final price privacy calculation stage, the two-party secure computing algorithm is improved and the three-party secure computing algorithm is realized, which is well adapted to the comparison among the current highest price, the current second highest price and the newly proposed bid of Vickery auction.

Finally, in order to evaluate the fairness performance quantitatively, a linear evaluation model of bidding mechanism is constructed for privacy protection and bidding income, and the weight parameters of the model are adjusted according to the existing methods. Through experiments, the proposed fairness protection method of Vickery auction has good fairness compared with the existing methods.

## References

1. Fang, W., Yao, X., Zhao, X., Yin, J., Xiong, N.: A stochastic control approach to maximize profit on service provisioning for mobile cloudlet platforms. IEEE Trans. Syst. Man Cybern.: Syst. **48**(4), 522–534 (2016)
2. Vickrey, W.: Counterspeculation, auctions, and competitive sealed tenders. J. Financ. **16**(1), 8–37 (1961)
3. Athey, S., Bagwell, K., Sanchirico, C.: Collusion and price rigidity. Rev. Econ. Stud. **71**, 317–349 (2004)
4. Ockenfels, A., Roth, A.E.: Late and multiple bidding in second price internet auctions: theory and evidence concerning different rules for ending an auction - sciencedirect. Games Econ. Behav. **55**(2), 297–320 (2006)
5. Yang, L., Li, C., Cheng, Y., Yu, S., Ma, J.: Achieving privacy-preserving sensitive attributes for large universe based on private set intersection. Inf. Sci. **582**, 529–546 (2022)
6. Yang, L., Li, C., Wei, T., Zhang, F., Ma, J., Xiong, N.: Vacuum: an efficient and assured deletion scheme for user sensitive data on mobile devices. IEEE Internet Things J. (2021)
7. Suzuki, K., Yokoo, M.: Secure generalized Vickrey auction using homomorphic encryption. In: Wright, R.N. (ed.) FC 2003. LNCS, vol. 2742, pp. 239–249. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45126-6_17

8. Sekhavat, Y.A., Fathian, M.: Efficient anonymous secure auction schema (ASAS) without fully trustworthy auctioneer. Inf. Manage. Comput. Secur. **16**(3), 288–304 (2008)
9. Al-Manthari, B., Nasser, N., Hassanein, H.: Congestion pricing in wireless cellular networks. IEEE Commun. Surv. Tutor. **13**(3), 358–371 (2011)
10. Zhang, X., Zhang, B., An, K., Chen, Z., Guo, D.: Auction-based secondary relay selection on overlay spectrum sharing in hybrid satellite-terrestrial sensor networks. Sensors **19**(22), 5039 (2019)
11. Sitz, M.B., Calkins, R.C., Feuz, M.D., Umberger, J.W., Eskridge, M.K.: Consumer sensory acceptance and value of wet-aged and dry-aged beef steaks. J. Anim. Sci. **84**, 1221–1226 (2006)
12. Jain, V., Panchal, G.B., Kumar, S.: Universal supplier selection via multi-dimensional auction mechanisms for two-way competition in oligopoly market of supply chain. Omega **47**(sep.), 127–137 (2014)
13. Li, C., Yang, L., Ma, J.: A secure and verifiable outsourcing scheme for assisting mobile device training machine learning model. Wirel. Commun. Mob. Comput. **2020** (2020)
14. Yi, B., et al.: Deep matrix factorization with implicit feedback embedding for recommendation system. IEEE Trans. Industr. Inf. **15**(8), 4591–4601 (2019)
15. Lin, B., et al.: A time-driven data placement strategy for a scientific workflow combining edge computing and cloud computing. IEEE Trans. Industr. Inf. **15**(7), 4254–4265 (2019)
16. Hahn, A., Singh, R., Liu, C.C., Chen, S.: Smart contract-based campus demonstration of decentralized transactive energy auctions. In: Power & Energy Society Innovative Smart Grid Technologies Conference (2017)
17. Jian, W., Qianggang, W., Niancheng, Z., Yuan, C.: A novel electricity transaction mode of microgrids based on blockchain and continuous double auction. Energies **10**(12), 1971 (2017)
18. Galal, H.S., Youssef, A.M.: Verifiable sealed-bid auction on the ethereum blockchain. In: Zohar, A., et al. (eds.) FC 2018. LNCS, vol. 10958, pp. 265–278. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-662-58820-8_18
19. Raziel, S.D.: Private and verifiable smart contracts on blockchains. Raziel': chastnyye i proveryayemyye smart-kontrakty na blokcheynakh (2018)
20. Hobbs, E.A., Benjamin, F.: Evaluation of a truthful revelation auction in the context of energy markets with nonconcave benefits. J. Regulatory Econ. **18**(1), 5–32 (2000)
21. Chen, J., Huang, H., Kauffman, R.J.: A public procurement combinatorial auction mechanism with quality assignment. Decis. Support Syst. **51**(3), 480–492 (2011)
22. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Cryptography Mailing list (2009). https://metzdowd.com
23. Yao, A.C.: Protocols for secure computation. In: Symposium on Foundations of Computer Science (1982)
24. Myerson, R.B.: Optimal auction design. Discuss. Pap. **6**(1), 58–73 (1981)
25. Wang, Y., Cai, Z., Yin, G., Gao, Y., Tong, X.: An incentive mechanism with privacy protection in mobile crowdsourcing systems. Comput. Netw. **102**, 157–171 (2016)
26. Sandholm, T.: Algorithm for optimal winner determination in combinatorial auctions. Artif. Intell. **135**(1–2), 1–54 (2002)
27. Zimmermann, H.-J.: Fuzzy programming and linear programming with several objective functions. Fuzzy Sets Syst. **1**, 45–55 (1978)

28. Snijders, T.A.B., Dormaar, M., Schuur, W.H.V., Dijkman-Caes, C., Driessen, G.: Distribution of some similarity coefficients for dyadic binary data in the case of associated attributes. J. Classif. **7**(1), 5–31 (1990)
29. Mookherjee, D., Reichelstein, S.: Dominant strategy implementation of Bayesian incentive compatible allocation rules. J. Econ. Theory **56**, 378–399 (1992)
30. Hastings, M., Hemenway, B., Noble, D., Zdancewic, S.: SoK: general purpose compilers for secure multi-party computation. In: 2019 IEEE Symposium on Security and Privacy (SP) (2019)
31. Asgharzadeh, Y., Fathian, M.: A newly high secure auction protocol without full-trusted auctioneer. In: Proceedings of 4th Iranian Society of Cryptology Conference, pp. 39–46 (2020)
32. Shachat, J., Wei, L.: Procuring commodities: first-price sealed-bid or English auctions? Mark. Sci. **31**, 317–333 (2012)
33. Cruciani, G., Baroni, M., Clementi, S., Costantino, G., Riganelli, D., Skagerberg, B.: Predictive ability of regression models. part i: standard deviation of prediction errors (SDEP). J. Chemom. **6**(6), 335–346 (1992)
34. Eichner, T., Wagener, A.: Multiple risks and mean-variance preferences. Oper. Res. **57**(5), 1142–1154 (2009)
35. Wang, X., Gao, Z., Guo, H.: Delphi method for estimating uncertainty distributions. Int. J. Inf. **15**(2), 449–460 (2012)