An anonymous and fair auction system based on blockchain

Zongli. Ye
Xiamen University of Technology
Chin-Ling Chen (clc@mail.cyut.edu.tw)
Chaoyang University of Technology
Wei Weng
Xiamen University of Technology
Hongyu Sun
Jilin Normal University
Woei-Jiunn Tsaur
National Taipei University
Yong-Yuan Deng
Chaoyang University of Technology

Research Article

Keywords: English auction, Blockchain, Ring Signature, Privacy Protection, Fairness

Posted Date: September 20th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2064583/v1

An anonymous and fair auction system based on blockchain

Zongli.Ye[1] Chin-Ling Chen[2,3],* Wei Weng[1], Hongyu Sun[4,5] Woei-Jiunn Tsaur [6,7] Yong-Yuan Deng[3,*]

[1] School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China
[2] School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China
[3] Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung City 413310, Taiwan
[4] Department of Computer Science, Jilin Normal University, Siping 136000, China
[5] State Key Laboratory of Numerical Simulation, Siping 136000, China
[6] Computer Center, National Taipei University, New Taipei City 237303, Taiwan
[7] Department of Computer Science and Information Engineering, National Taipei University, New Taipei City 237303, Taiwan

* Correspondence: clc@mail.cyut.edu.tw (C.-L.C.); allen.nubi@gmail.com (Y.-Y D.)

Abstract

Transaction volumes are growing rapidly, demonstrating how well-liked online auctions are with shoppers. Bidders can access a wider variety of products and sellers can reach a larger audience through online auction platforms. However, privacy concerns have reduced users' trust in auction platforms, and difficult disputes have caused consumers to question the fairness of online auctions, negatively impacting the market growth. The emergence of blockchain technology has brought a new approach to solving these problems. Blockchain is a new generation of information technology that is decentralized, transparent, traceable, anti-tampering, and unforgeable, following big data, cloud computing, and artificial intelligence. In this paper, we present a blockchain-based online auction solution as well as an auction protocol that uses ring signatures to guarantee anonymity. Three features summarize this essay: (1) Making use of blockchain technology to ensure that the auction transaction process is transparent, traceable, tamper-proof, and unforgeable. (2) The ring signature-based anonymous auction protocol allows for the concealment of bidders' public keys in a group of public keys. Because malicious individuals are prevented from evaluating data by tracking numerous transactions of a single public key, this significantly protects the privacy of bidders. (3) The proposed scheme promotes auction fairness and effectively resolves disputes.

Keywords: English auction, Blockchain, Ring Signature, Privacy Protection, Fairness

1. Introduction

1.1 Background

With the prevalence of e-commerce, shopping online has become the main shopping method for consumers due to the convenience of online transactions. The use of English auctions, one of the most popular auction methods available, would help the seller receive greater returns than with other auction models. Online auction transactions have grown dramatically in recent years. According to research by ArtTactic [1], online auction sales for Christie's, Sotheby's, and Phillips reached $1.35 billion in 2021, up 28.2% from 2020 and accounting for 10.7% of total auction sales. For these three businesses, Internet sales in 2019 totaled just $168.2 million, with an exponential growth rate. And the combined online sales for these three companies in 2019 were only $168.2 million. Estimates suggest that between 2021 and 2026, the value of the online auction industry will expand by an extra $1.9 billion, which is a very positive expectation.

But because of all the attention, there are many problems with the online auction market, such as issues with fraud, user privacy, and fair trade. As an example, merchants that utilize phony bidder identities to make higher winning bids on their auctioned items may exploit rule loopholes to their benefit. A further situation has two bidders participating in an auction concurrently, one submitting a low offer and the other a very high one. The top bidder gives up the bid as the auction comes to a close, which causes the low bid to be accepted as the winning bid. It is abundantly clear from PR Newswire's study [2] that concerns about fraud may limit the market growth. Sincere

participants are more concerned about protecting their privacy and getting treated fairly. Fairness is prioritized by participants in the bidding process, and unbiased activity enables bidders to obtain lots at a reasonable cost. Certainly, utilizing a third party or applying reasonable regulations can improve fairness. Therefore, sincere bidders are more worried about suffering unnecessarily as a result of the revealing of personal information. This worry is necessary considering that industry giant Google recently had its usage of Google Analytics, a tool for data analytics that can track millions of users and gather data on a variety of users, banned[3][4]. In the well-established Internet economy, user data has a very high value. To gain more from it, malicious people may use analytics tools to hunt down personal information about users' hobbies and financial situations by analyzing their transaction data.

Fairness and anonymity have always been the two most important elements in an auction. For an auction to be fair, both the rules and the information given to bidders must be fair, consistent, and transparent. Participants must provide as little personal information as possible throughout the auction process to preserve anonymity and avoid exploitation.

The following are some important claim priorities in the auction process, as determined by studies [5,6,7].

(1) Information about bid transactions should not be managed centrally, but rather transparently and securely.
(2) Both the winning bidder's legitimacy and the winning bid's legitimacy may be independently verified.
(3) The owner is not permitted to pretend to be a bidder and place bids on its own provided things.
(4) When sellers and bidders disagree with a transaction, there are acceptable and transparent methods to handle the situation.
(5) There is an appropriate way to deal with malicious bidders.

Naturally, a well-designed auction system should be extremely effective and practical to operate. Therefore, a public English online auction system should satisfy the following requirements to preserve blockchain properties and security issues.

(1) Data Integrity [5]: Fairness depends on data integrity, and data integrity should be verified.
(2) Unforgeability[5, 8, 9, 10]: Protect the willingness of the bidders and make sure dishonest bidders cannot enter the auction by pretending to be someone else and forging the signatures of other bids.
(3) Non-repudiation[5, 8, 9]: The successful bidder cannot contest his position as the winning bidder.
(4) Traceability[5, 8, 9, 10]: After the auction is over, the winning bidder may be traced to finish the transaction, such as payment.
(5) Verifiability[5, 8, 9, 10]: The legitimacy of the bidder, the validity of the offer, and the accuracy of the winner's announcement may all be independently checked by the public.
(6) Easy revocation[5, 8, 9]: When a bidder is suspected of being dishonest, the platform can withdraw their bid.
(7) Anonymity[5, 8, 9, 10]: The bidder cannot be determined from the bid information by either auctioneers or bidders.
(8) Fairness[5, 8, 9, 10]: The bidders' issues are addressed properly, and the auction is performed fairly.
(9) Resist Known Attacks[5, 10]: The online auction system should be able to resist attacks to ensure the robustness of the system.

Systems that comply with the requirements listed are regarded as workable and generally fair. It is crucial to meet these needs and deal with the difficulties to promote the healthy development of the whole auction industry. The majority of the problems with the auction process have been fixed[8, 9, 11, 12], and some progress has been made toward user anonymity. As Lee et al.[6] pointed out, it still falls short of what is needed for online auctions since centralized auctions have several drawbacks and the centralized method still faces numerous objections. In response to the issues highlighted above, a new architectural design paradigm for online auctions has risen with the emergence of blockchain technology.

People began to pay attention to the distributed ledger technology that underpins Bitcoin after its meteoric rise in popularity in 2008. This distributed ledger system, which was eventually given the moniker blockchain technology, is decentralized and tamper-proof [13]. The blockchain platform conduct transactions using their private and public keys without disclosing their actual identities, and they can utilize cryptographic techniques, hashing algorithms, digital signatures, and other technologies to ensure that the transferred data are not tampered with. The record cannot be changed again when the transaction information is published to the blockchain, and each transaction detail is traceable. The adoption of blockchain technology can address issues with user

privacy, fraud, and fair transactions in online auctions. Numerous academics have researched the use of blockchain in online auctions[5, 6, 7, 10, 14, 15, 16]. The use of blockchain in auctions increases people's trust and enthusiasm for online auctions. However, even if users only use their public and private keys for transactions, it has been demonstrated that privacy breaches may happen in blockchain [17]. Despite the user address in the blockchain being pseudonymous, it is still feasible to connect it to the user's true identity because numerous users frequently use the same address for transactions. Therefore, the focus of the study on the subject of online auctions has shifted to how to enhance user anonymity in blockchain-based online auction systems.

The blockchain auction system put out in this work meets the requirements[5, 8, 9, 10] in addition to having the following features.

(1) The auction mechanism is made more effective by the Schnorr digital signature approach.
(2) The anonymity of participants is completely safeguarded by the proposed anonymous auction protocol technique, which is based on ring signatures.
(3) Transparency in the transaction process is increased by decentralized blockchain technology.
(4) Previous research has often given the settlement of disputes during the auction process little attention, which lessens the fairness of the auction. In this study, we suggest a straightforward dispute resolution method that supports the fairness of the auction process.

1.2 Related Works

Online auction research has mostly focused on privacy and fairness. Before 2008, [8, 9, 11, 12] used a variety of methods to preserve user privacy. Lee et al.[8] made the assumption that the registered manager and auction manager won't conspire to compromise bidder anonymity, performs a randomization operation during the bidding process to protect winner anonymity, enhances information transparency, and ensures public verifiability by posting all pertinent information on a bulletin board. By using an elliptic curve cryptosystem, Chen minimized the time that bidders must spend waiting for auction certificates to be issued, improved bidder efficiency, and made the auction efficient and simple to execute [9]. Chang et al.[11] protected the bidders' anonymity by employing the deniable authentication technique[18]. However, Jiang et al.[12] pointed out that the anonymous protocol had security flaws, and a malevolent individual might disable the auction phase by forcing bidders and auctioneers to use separate keys. The safe mutual authentication in the protocol between bidders and auctioneers is improved. These studies are all based on the centralized server system. People are still concerned about if the transaction data will be tampered with and whether the transaction procedure is fair.

After 2008, the emergence of blockchain technology opened up new study paths for online auctions. Scholars have investigated the integration of blockchain into online auctions [5, 6, 7, 10, 14, 15, 16], with some success. Xiong et al.[10] presented a revocable ring signature-based conditional privacy-preserving auction protocol in which only RM(Registration manager) and AM(Auction manager) work together to expose the true bidder. Chang et al.[5] presented an auction protocol based on the elliptic curve cryptosystem (ECC) and identified design faults and vulnerability to denial-of-service attacks in [10]. This auction protocol doesn't have a transparent transaction process and depends on a reliable Agent Center. Braghin et al.[14] demonstrated how to construct several auction types on basis of the Ethereum blockchain while ensuring data integrity, openness, and non-repudiation. The approach, however, lacks transaction privacy and is pseudo-anonymous, as the authors lament. Enkhtaivan et al.[15] presented an anonymous English auction mechanism based on group signatures with trusted hardware and blockchain, where group signatures secure user identities and the trusted hardware environment assures that group administrators do not have additional breaches. But there is no examination of how disagreement situations are handled in the scheme. Lee et al.[6] used smart contracts and reputation algorithms to develop new auction protocols on blockchain networks, but a key flaw in the plan is that it does not prioritize user privacy. By limiting participant coalitions, Qusa et al.[16] sought to improve the e-auction system of UAE(United Arab Emirates), however, the protocol fell short of anonymity and unlinkability. Huang et al.[7] offered an anonymous bidding protocol that uses R-LRRS ring signatures to ensure anonymity, lowers disagreements through two-way confirmation, and prevents the development of dishonest bids by asking players to pay a deposit. We agree with the author's assertion that the method achieves undeniability, but dispute-freeness is not the same thing as undeniability. How disagreements are resolved is not stated in the proposed scheme, particularly if the vendor is at fault. Therefore, we think that the agreement still has an opportunity for development.

The related studies[5, 6, 10, 14, 15, 16, 18] have been crucial in advancing the online auction market and guiding it in the expected direction. Table 1 shows the comparison between the existing online English auction schemes.

Table 1. Comparison between the proposed and existing online English auction Schemes.

Authors	Year	Objective	Technologies	Merits	Demerits
Xiong et al.[10]	2012	A revocable ring signature-based conditional privacy-preserving auction protocol.	Revocable ring signature	The user's identity is concealed via ring signature, and only RM and AM work together could expose the real signer.	No blockchain is utilized. Chang et al.[5] noted that the protocol is vulnerable to DoS Attacks.
Chang et al.[5]	2013	A protocol based on the Elliptic Curve Cryptosystem (ECC).	ECC	A dispute stage is added to deal with disputes in the auction.	The lack of a blockchain, the lack of transparency in the transaction process, and the need for a reliable Agent Center are all disadvantages.
Braghin et al.[14]	2018	While analyzing the cost of constructing prototypes for four typical auctions, the authors demonstrated how to create bidding on Ethereum.	Blockchain, Smart Contracts	It realized the transparency and non-repudiation of the auction and ensured the integrity of the data	The application lacks transaction privacy and is regarded as pseudo-anonymous.
Enkhtaivan et al.[15]	2019	A Trusted Hardware-based and blockchain-based anonymous English auction scheme.	Blockchain, Group Signature	The hardware-based Trusted Execution Environment (TEE) ensures that group administrators do not have other violations.	The program doesn't examine how disputes are resolved.
Lee et al.[6]	2020	It developed a new auction mechanism on the blockchain network using smart contracts and reputation management.	Blockchain, Smart Contracts	Without relying on third parties, it ensured fair transactions and increase dependability by incorporating blockchain's tamper-proof and decentralized.	This protocol paid no attention to user privacy and did not analyze how disputes were handled.
Qusa et al.[16]	2020	The e-auction system is to be improved by a blockchain-based system that forbids participant partnerships.	Blockchain, Smart Contracts	Confidentiality was ensured via blockchain.	Neither anonymity nor unlinkability was attained.
Huang et al.[7]	2021	A two-way anonymous bidding protocol using R-LRRS ring signatures.	R-LRRS ring signature, policy-driven chameleon hash	The R-LRRS ring signatures enabled users' anonymity. Reducing the presence of rogue bidders via deposits.	The program is not entirely free of controversy.

The summary analysis led to the following three conclusions.

(1) The methods[5, 10] are vulnerable to DoS attacks and lack auction transaction transparency since they don't make use of blockchain technology.
(2) Methods[6, 14, 16] either don't care about user privacy or don't protect transactional privacy when pseudo-anonymous users are involved.
(3) The schemes' [7, 15] unclear dispute resolution procedures weaken the fairness of the auction process.

The remainder sections are described as follows: Section 2 focuses on the methods applied in our suggested approach. Our precise plan and the whole procedure are presented in Section 3. The pertinent characteristics of this design are examined and discussed in Section 4. The computation cost and communication cost are covered in Section 5 along with comparisons to other schemes. Finally, we provide a summary in Section 6.

2. Preliminary

2.1 Blockchain Technology

Decentralization, Persistency, Anonymity, and Auditability are recognized as fundamental characteristics of blockchain technology and are seen to have the potential to revolutionize established sectors[19][20]. Blockchain technology is predicted to successfully tackle the trust problem in network communication. Without a central trust middleman, mutually misinformed parties perform secure transactions in blockchain applications. Without a central trusted middleman, mutually misinformed parties trade securely in blockchain applications.

Blockchain is the underlying technology that underpins Bitcoin. It was suggested by Satoshi[21] in 2008 and implemented on Bitcoin in 2009, as a new technique for storing, transmitting and controlling information. A blockchain[22] is a collection of interconnected blocks that functions as a typical public ledger by maintaining an exhaustive list of transaction data. Due to its distributed nature, blockchain can prevent single points of failure. Because a blockchain is immutable, a transaction that has been bundled into one cannot be changed after that. Through the created addresses, users interact with blockchain apps, and the anonymity based on hash cryptography may effectively safeguard user privacy and demonstrate uniqueness. People not trusting each other can be resolved thanks to the fact that blockchain records information that is more authentic and trustworthy than information on traditional networks.

2.2 Inter Planetary File System（IPFS）

While online auction systems typically require displaying the photos or indeed video of lots, storing huge images in the blockchain is a challenge. Using IPFS to store information about lots helps enhance the operating efficiency of online auctions.

A peer-to-peer (P2P) storage network, IPFS is a new kind of storage technology [23]. The IPFS[24, 25] is a distributed file system that was created to address the issue of excessive file redundancy. Assigning a different hash value to each file, IPFS is a decentralized and shared storage technology to divide files into several pieces that are stored on each network node. A lot of storage space is saved since there will only be one duplicate of a file with identical information in the system. The fundamental advantage of IPFS is that access may be made possible using content-based addressing rather than location-based addressing. Additionally, multi-node storage significantly lowers the chance of data loss.

2.3 The signature scheme proposed by Schnorr

In 1989, Schnorr[26] introduced a discrete logarithm-based signature method that, because of its shorter signature length and quick signature generation, garnered a lot of attention. These two features make the signature algorithm highly attractive to application developers. Several Schnorr-based signature methods[27, 28] have been developed by academics to improve Bitcoin's efficiency and user privacy, and the Bitcoin community is contemplating implementing the Schnorr signature algorithm[29]. We should eagerly anticipate the practical implementation of the Schnorr signature algorithm.

The procedure for generating a Schnorr signature includes three steps.

Define p and q are large prime numbers, $p \mid q-1$. Make $q \geq 2^{140}$ and $p \geq 2^{512}$. g is the element in Z_p and $g^q = 1 \bmod p$ (q is the order of Z_p, $g \neq 1$).

(1) Key generation.

(a) Select a random number $x\left(1 < x < q\right)$ as a private key.

(b) Calculate the public key $y = g^x \bmod p$.

(2) Generate signature for message m.

(a) Choose a random number $k\left(1 < k < q\right)$.

(b) Calculate $c = h\left(m, g^k \bmod p\right)$.

(c) Calculate $s = k + xc \bmod q$.

(d) Take signature $\left(c, s\right)$ as an output.

(3) Verify Signature.

(a) Calculate $e = g^s y^c \bmod p$.

(b) Check the equation $c \stackrel{?}{=} h\left(m, e\right)$. The signature is valid if the equation holds, and invalid if it does not.

2.4 AOS（Abe-Ohkubo-Suzuki）Ring Signature

Blockchain has a lot of potentials, but it also has several difficulties. Studies[17, 30] demonstrated that following users' bitcoin transactions can expose personal information about them, and the blockchain cannot completely ensure transaction privacy[31]. Ring signatures can be a useful solution to this problem.

Rivest et al.[32] initially introduced a signature technique known as a ring signature algorithm that may conceal the identity of the true signer while yet granting the signer absolute anonymity. Ring signatures don't have management like group signatures do, hence there is no chance of the manager selling the true signer's personal information. Additionally, ring signatures are self-organizing structures that allow the genuine signer to autonomously pick other public keys to create the ring signature. As a result, ring members do not need to join or leave a group in advance. Since ring signatures are more anonymous than group signatures, they are the best option for scenarios in which users need to hide their true identities.

The real signer signs the file using both its private key and the public keys of the other members in the ring signature generation process after selecting a random set of members (including itself) as potential signers. There are three primary algorithms used in this procedure.

$Gen\left(k\right)$: Enter the security parameters k and $Gen\left(k\right)$ generates a public-private key pair $\left(y_i, x_i\right)$ for each user.

$Sign\left(m\right)$: Select a set of public keys to build the public key set L, $L = \left(y_1, y_2, \mathrm{L}\ , y_s, y_{s+1}, \mathrm{L}\ , y_n\right)$.

$Sign\left(m\right)$ outputs a signature R for the message R using the signer's private key x_s.

$Verify\left(m, R\right)$: By confirming that the equations are equal, the $Verify\left(m, R\right)$ returns "True" or "False." The signature R is valid if the output is "True," and invalid if it is "False."

One-way trapdoor-based public key mechanisms (e.g., RSA) or discrete logarithm puzzle-based public key structures can both make use of the AOS ring signature[33]. The AOS ring signature offers strong operational performance in addition to exceptional anonymity.

Assume that the user U_k has a private key x_k and public key y_k ($y_k = g^{x_k} \bmod p$). L is the set of $n-1$ public keys (including y_k). $h(\ )$ is a publicly available hash function.

The user generates an AOS ring signature by following these steps.

(1) Select $\alpha \in Z_q$ and calculate $C_{k+1} = \left(L, m, g^\alpha \bmod p\right)$.

(2) Forming a positive sequence, choose $s_i \in Z_q$ and calculate $C_{i+1} = h\left(L, m, g^{s_i} y_i^{C_i} \bmod p\right)$.

(3) Calculate $s_k = \alpha - x_k C_k \bmod q$ to close the ring.

(4) Put $\sigma = \left(C_0, s_0, s_1, \mathrm{L}\ , s_{n-1}\right)$ as a signature.

The user verifies the ring signature by following these steps.

(1) Calculate $e_i = g^{s_i} y_i^{C_i} \bmod p$ and $c_{i+1} = h\left(L, m, e_i\right)$.

(2) Determine if the equation $C_0 \stackrel{?}{=} h(L, m, e_{n-1})$ holds. If it holds, output "Accept", otherwise output "Reject".

3. The Proposed Scheme

3.1 System Model

Figure 1 shows an overview of the online auction framework, with the key participants being OAP (Online Auction Platform), DA (Dispute Arbitrator), SL (Sellers), and BR (Bidders).

(1) **OAP**: It serves as an "intermediary" between sellers and bidders by providing a platform for sellers to exhibit auction items and a platform for bidding to bid. The following are the OAP's responsibilities: validating the sellers' and bidders' participation rights before the auction, announcing the winner's public key after the auction, and punishing malicious bidders after the auction.

(2) **DA**: The DA is in charge of resolving complaints throughout the auction process and making fair judgments, making the auction system more fair and controlled.

(3) **SL**: SL is a trustworthy user who is looking to sell precious stuff. Bids cannot be initiated by SL who are not registered.

(4) **BR**: BR is users who have been allowed entry to the auction. Participants who have not registered are unable to bid in the auction.

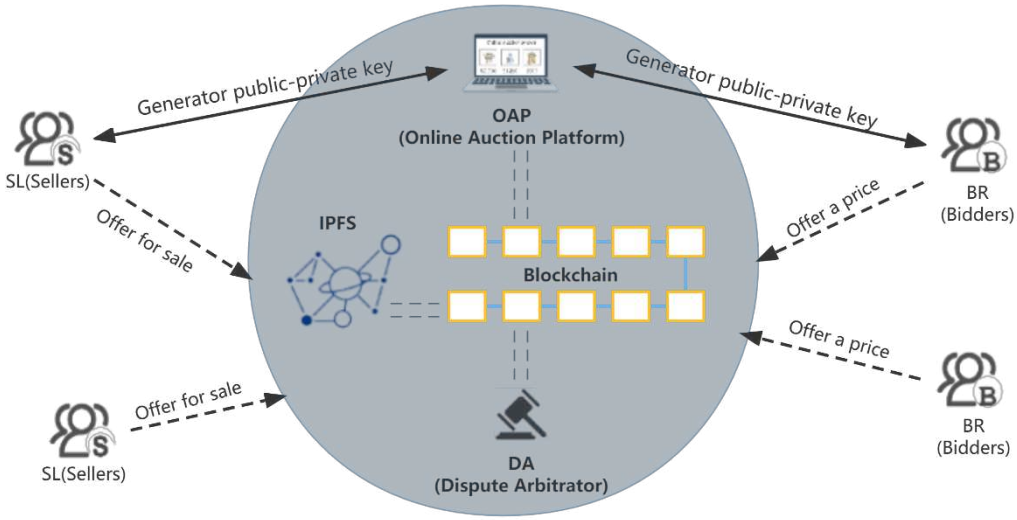

Figure 1. Overview of online auction framework.

3.1.1 Online Auction Procedure

This paper is divided into five phases, which are Initialization Phase, Pre-auction Phase, Auction Phase, Announce winner Phase, and Dispute Resolution Phase. Following SL and BR's submission of the required data to KGC to end the Initialization Phase, Figure 2 depicts the bidding procedure. Additionally, as online bidding is frequently the topic of contentious circumstances, we will go into more detail on this in section 3.6.

Initialization Phase: The user supplies the information required to finish the registration process and receives the public and private keys.

Pre-auction Phase: To continue bidding in the auction, SL and BR must each complete a formal pre-bidding check.

Auction Phase: BR increases the price to enhance his chances of winning the desired products.

Announce Winner Phase: At this point, OAP declares the auction winner.

Dispute Resolution Phase: At this phase, SL or BR can express concerns about bid anomalies, and DA will handle the case and announce the results.

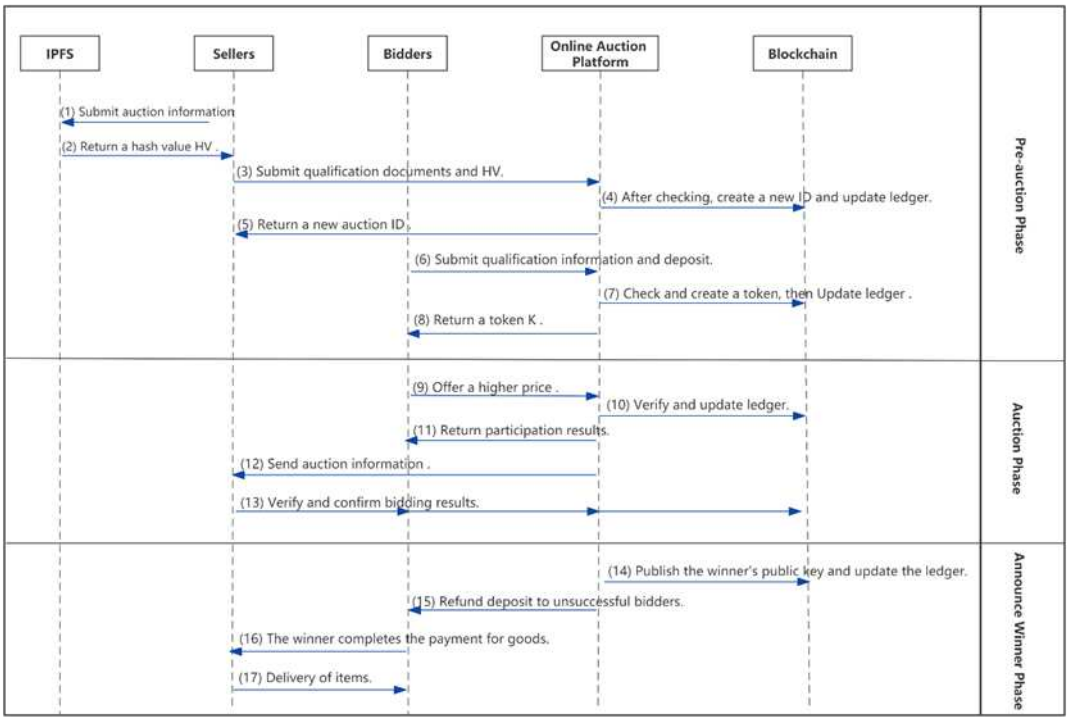

Figure 2. The proposed auction procedure.

3.1.2 System Architecture Diagram

This plan utilizes blockchain and ring signatures to develop a tamper-proof, supervisable, and traceable online auction system. The application layer, extension layer, protocol layer, and storage layer are the layers that make up the online auction system's layered architecture, as shown in Figure 3.

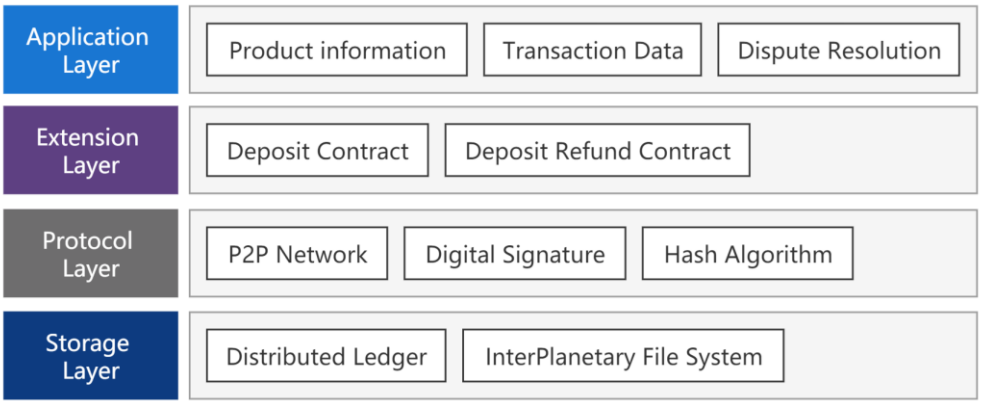

Figure 3. Diagram of the layered architecture for online auction.

(1) **Application Layer**: Displaying multiple auction situations at the application layer. Through the application interface, users may access information and statistics about auction products and manage appeals for disputes.

(2) **Extension Layer**: In the extension layer, we can not only enrich the functions of the auction system but also drive the business to run efficiently through smart contracts. Through smart contracts, which are in charge of defining the specifics of how transactions are made and the process, some predefined rules and terms can have their implementation automated. Before the auction is executed, the deposit must be paid according to the rules of the Deposit Contract, and once the auction is completed, the deposit can be refunded according to the terms of the Deposit Refund Contract.

(3) **Protocol Layer**: P2P network networking, a digital signature mechanism, and a hash algorithm are integrated at the protocol layer to create a peer-to-peer, secure, and reliable network and communication foundation for the upper layer.

(4) **Storage Layer**: Keep the data files generated and required by the programs running on the upper layer. The distributed ledger holds information about auction transactions, while the IPFS file system keeps information on how auction products are displayed, including images, audio, and video.

3.2 Initialization phase

Any user who wishes to utilize the system must provide the required identification data M_1 to OAP to complete the initialization. OAP then distributes the public and private keys to users. The data flow diagram for the Initialization phase is shown in Figure 4.

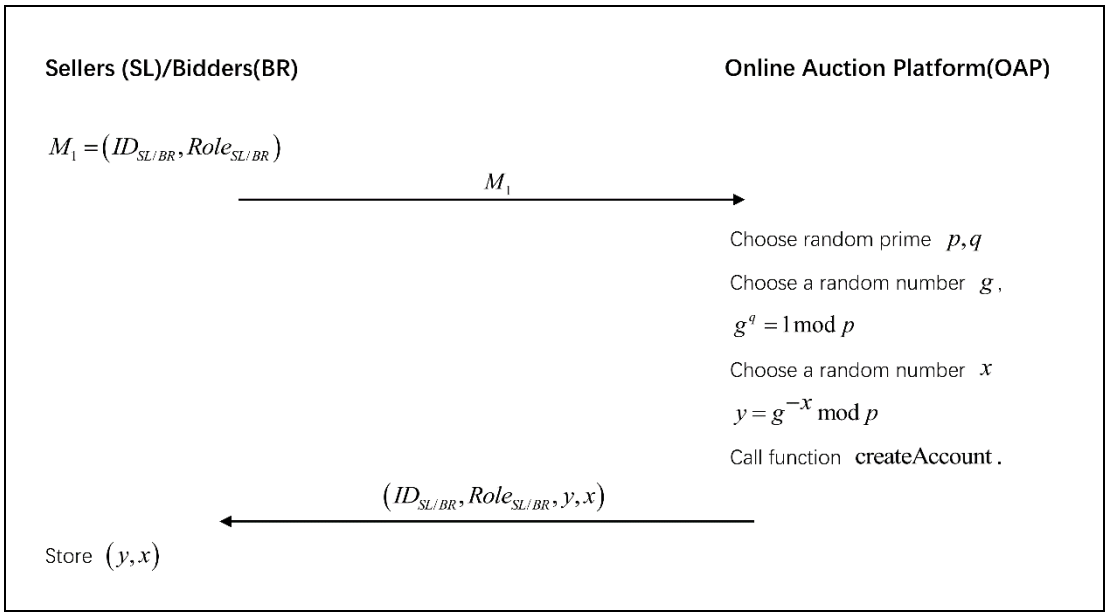

Figure 4. Initialization phase

Step 1. SL/BR submits identity information $ID_{SL/BR}$ and role information $Role_{SL/BR}$ to OAP.

$$M_1 = (ID_{SL/BR}, Role_{SL/BR}) \tag{1}$$

Step 2. OAP generates system parameters (g, p, q). The relationship between these three parameters is as follows,

$$g^q = 1 \bmod p \tag{2}$$

Then OAP chooses a random parameter $x(1 < x < q)$ as the private key of the applicant. And call the function $createAccount(ID_{SL/BR}, y, Role_{SL/BR})$ to create user information after calculating the public key y via equation (3).

$$y = g^{-x} \bmod p \tag{3}$$

The protocol for creating a new account is given in **Algorithm 1**.

Algorithm 1. Create a new account.

```
Function createAccount(_id, _y, _role)
    If (_id || _y exist) then
        The _id or _y has been used before.
    Else
        _userInfo < -New userInfo(char ID, char pk, char role, boolean punished:false, boolean
credit: "low", array qualifyInfo: []);
        _userInfo[ID] < - _id;
        _userInfo[pk] < - _y;
        _userInfo[role] < - _role;
    End if
    Return _userInfo;
```

3.3 Pre-auction Phase

During this phase, there are two aspects of work that need to be completed. One is that SL requests OAP to initiate an auction, and OAP checks the lot's details SL provided. Figure 5 presents the data flow diagram for the application by SL to start a new auction. Second, BR presents a request to OAP to take part in the auction, and OAP examines the information BR provided on the deposit transaction and credit score. Details are shown in Figure 6.

The signature function $Sig(\ )$ is described in **Algorithm 2**, and the algorithm $verSig(\ )$ for verifying signatures is described in **Algorithm 3**. The algorithm for SL to create new auctions is described in **Algorithm 4**. The algorithm for BR to obtain bidding privileges is described in **Algorithm 5**.

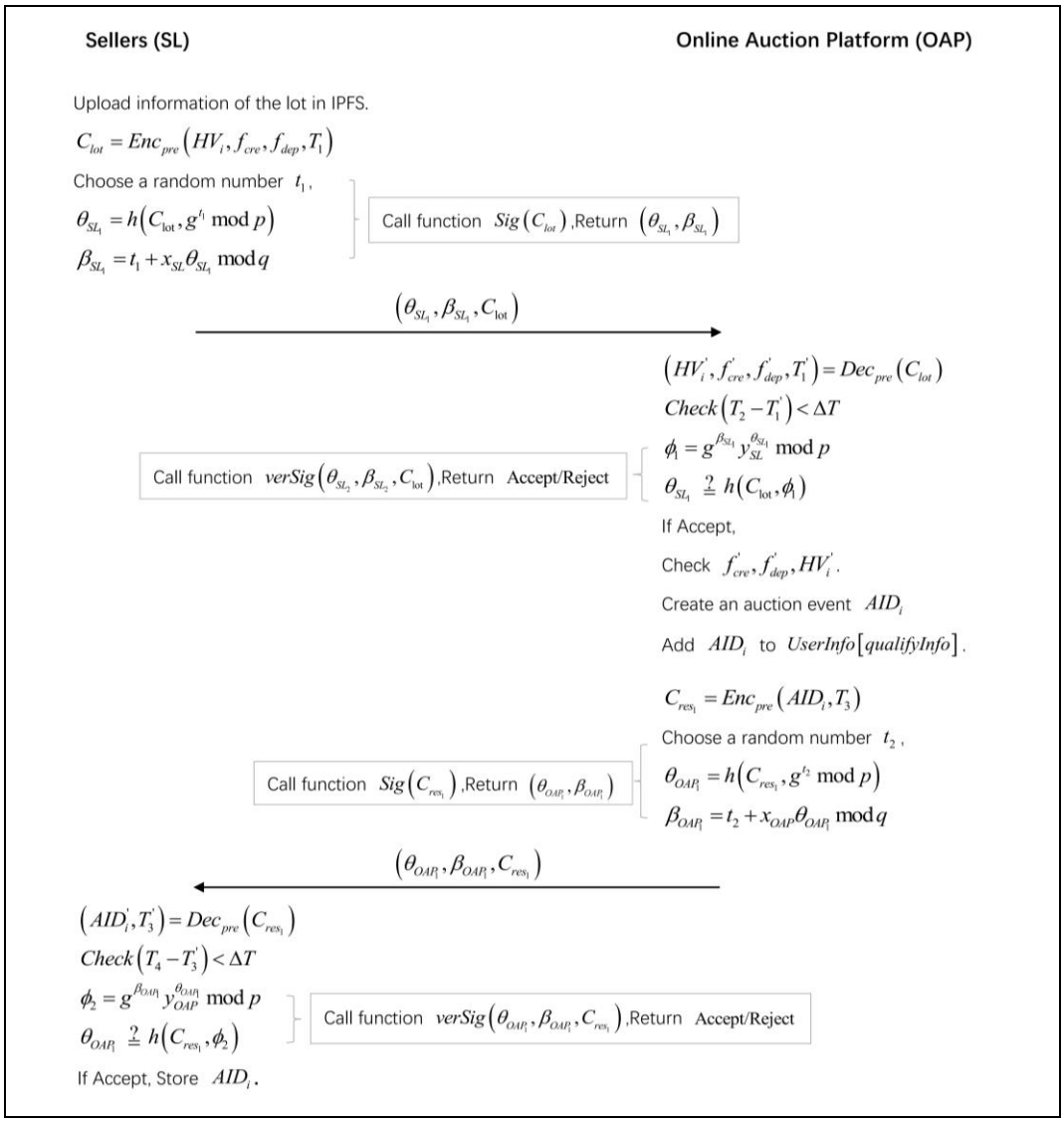

Figure 5. SL creates a new auction.

Here are the steps for starting a new auction.

Step 1. After successfully storing lots of information in IPFS, SL receives a hash value HV_i. Then, the required credibility values f_{cre} and the deposit requirements f_{dep} for qualified bidders as well as product information HV_i are encrypted.

$$C_{lot} = Enc_{pre}(HV_i, f_{cre}, f_{dep}, T_1) \tag{4}$$

The encrypted data C_{lot} is then signed using parameters t_1 chosen at random. SL delivers C_{lot} and signature $(\theta_{SL_1}, \beta_{SL_1})$ to OAP.

$$\theta_{SL_1} = h(C_{\text{lot}}, g^{t_1} \bmod p) \tag{5}$$

$$\beta_{SL_1} = t_1 + x_{SL}\theta_{SL_1} \bmod q \tag{6}$$

Step 2. OAP initially decrypts C_{lot} when it gets $\left(\theta_{SL_1}, \beta_{SL_1}, C_{\text{lot}}\right)$ from SL.

$$\left(HV_i^{'}, f_{cre}^{'}, f_{dep}^{'}, T_1^{'}\right) = Dec_{pre}\left(C_{lot}\right) \tag{7}$$

Then, make sure the timestamp is valid.

$$Check\left(T_2 - T_1^{'}\right) < \Delta T \tag{8}$$

Verify the signature when the timestamp is valid.

$$\phi_1 = g^{\beta_{SL_1}} y_{SL}^{\theta_{SL_1}} \bmod p \tag{9}$$

$$\theta_{SL_1} \stackrel{?}{=} h\left(C_{\text{lot}}, \phi_1\right) \tag{10}$$

If equation (10) is true, the signature is acceptable legally. Then check to see if the user has the role of "seller" before opening the auction. If $HV_i^{'}, f_{cre}^{'}, f_{dep}^{'}$ satisfy the standards, a new AID_i is created. Finally, OAP encrypts and signs AID_i as follows.

$$C_{res_1} = Enc_{pre}\left(AID_i, T_3\right) \tag{11}$$

Choose a number t_2 at random,

$$\theta_{OAP_1} = h\left(C_{res_1}, g^{t_2} \bmod p\right) \tag{12}$$

$$\beta_{OAP_1} = t_2 + x_{OAP}\theta_{OAP_1} \bmod q \tag{13}$$

Step 3. After receiving $\left(\theta_{OAP_1}, \beta_{OAP_1}, C_{res_1}\right)$, SL decrypts C_{res_1}.

$$\left(AID_i^{'}, T_3^{'}\right) = Dec_{pre}\left(C_{res_1}\right) \tag{14}$$

Then confirm the timestamp's validity.

$$Check\left(T_4 - T_3^{'}\right) < \Delta T \tag{15}$$

Verify the signature $\left(\theta_{OAP_1}, \beta_{OAP_1}\right)$ if the timestamp is valid.

$$\phi_2 = g^{\beta_{OAP_1}} y_{OAP}^{\theta_{OAP_1}} \bmod p \tag{16}$$

$$\theta_{OAP_1} \stackrel{?}{=} h\left(C_{res_1}, \phi_2\right) \tag{17}$$

The signature is accepted if equation (17) holds. With this AID_i, SL could enhance the lots' details by adding more photos or videos to make it more attractive.

The steps for BR to apply for participation in the auction are as follows.

Step 1. When BR transfers a deposit to OAP, a DID_i is generated. Then, BR encrypts $\left(AID_i, DID_i, T_5\right)$.

$$C_{BR} = Enc_{pre}\left(AID_i, DID_i, T_5\right) \tag{18}$$

BR chooses the parameters t_3 at random to sign the encrypted data C_{BR} and transmits $\left(\theta_{BR_1}, \beta_{BR_1}, C_{BR}\right)$ to OAP.

$$\theta_{BR_1} = h\left(C_{BR}, g^{t_3} \bmod p\right) \tag{19}$$

$$\beta_{BR_1} = t_3 + x_{BR}\theta_{BR_1} \bmod q \tag{20}$$

Step 2. OAP gets $\left(\theta_{BR_1}, \beta_{BR_1}, C_{BR}\right)$ and decrypts C_{BR} before validating the timestamp.

$$\left(AID_i^{'}, DID_i^{'}, T_5^{'}\right) = Dec_{pre}\left(C_{BR}\right) \tag{21}$$

$$Check\left(T_6 - T_5^{'}\right) < \Delta T \tag{22}$$

After confirming the timestamp is accurate, OAP checks the signature $\left(\theta_{BR_1}, \beta_{BR_1}\right)$.

$$\phi_3 = g^{\beta_{BR_1}} y_{BR}^{\theta_{BR_1}} \bmod p \tag{23}$$

$$\theta_{BR_1} \stackrel{?}{=} h\left(C_{BR}, \phi_3\right) \tag{24}$$

If equation (24) holds, then OAP checks the following three points.
First, check if the BR acts as a "bidder."
Second, check whether the BR's credit satisfies the essential requirements.

Lastly, confirm if the BR has paid the deposit via $DID_i^{'}$.

If all three terms are met, OAP offers the applicant a token K_i. Encrypt $AID_i^{'}$ and K_i,

$$C_{res_2} = Enc_{pre}\left(AID_i^{'}, K_i, T_7\right) \tag{25}$$

Then randomly select a number t_4 to sign C_{res_2} and send $\left(\theta_{OAP_2}, \beta_{OAP_2}, C_{res_2}\right)$ to BR.

$$\theta_{OAP_2} = h\left(C_{res_2}, g^{t_4} \bmod p\right) \tag{26}$$

$$\beta_{OAP_2} = t_4 + x_{OAP}\theta_{OAP_2} \bmod q \tag{27}$$

Step 3. BR decrypts the C_{res_2} and then verifies the validity of the timestamp.

$$\left(AID_i, K_i^{'}, T_7^{'}\right) = Dec_{pre}\left(C_{res_2}\right) \tag{28}$$

$$Check\left(T_8 - T_7^{'}\right) < \Delta T \tag{29}$$

After the verification of equation (29), make sure the signature is valid also.

$$\phi_4 = g^{\beta_{OAP_2}} y_{OAP}^{\theta_{OAP_2}} \bmod p \tag{30}$$

$$\theta_{OAP_2} \stackrel{?}{=} h\left(C_{res_2}, \phi_4\right) \tag{31}$$

When the patterns in equation (31) match, BR saves $K_i^{'}$ as a participation ticket which will be used in the Auction Phase.

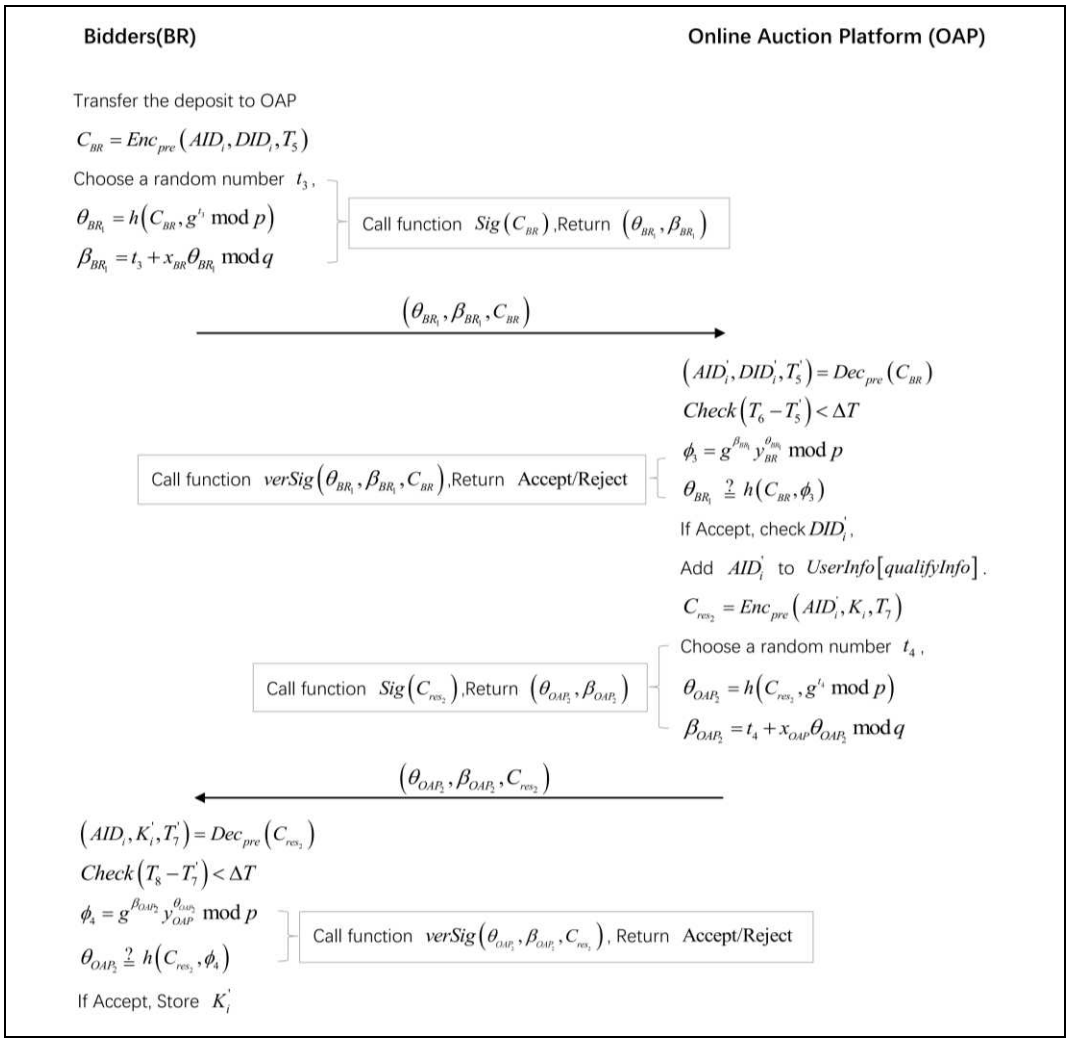

Figure 6. BR applies to participate in bidding.

Algorithm 2. Generate a signature.

```
Function Sig (m)
    Choose a random value t(1<t<q).
    Z= pow (g, y);
    Compute c <- h(m, Z mod p);
    Compute s <- t + x*c mod q;     /*x is private key of user*/
    Return (c, s)
```

Algorithm 3. Verify signature.

```
Function verSig (c, s, m)
    Compute V1 <- pow (g, s);
    V2<- pow (y, c);     /*y is public key of user*/
    e < - V1 * V2  mod p;
    if (c==h(m, e)) then
        Return Accept.
    else
        Return Reject.
    end if
```

Algorithm 4. SL creates an auction.

```
Procedure reqAuctionID (_goodInfo, _userInfo)
    if(_userInfo[role] == "seller") then
        OAP checks the goods information via _ goodInfo .
        if (Successful verification) then
            Create an auction event ID and add it to _userInfo[qualifyInfo].
            Return ID.
        else
            SL needs to offer more information to OAP.
        end if
    else
        The user cannot create a new auction item.
    end if
End Procedure
```

Algorithm 5. Bidders obtain bidding qualification.

```
Procedure reqParticipation(_userInfo,_auctionID,_paymentID)
    if(!_auctionID) return false;
        if(_userInfo[role] == "bidder") then
            if(_userInfo[credit] meets requirements) then
                Check _paymentID,
                If checked, add the _auctionID to _userInfo[qualifyInfo].
                Return a token k.
            else
                BR needs to offer more information to OAP.
            end if
        else
            BR is unable to participate in an auction as a buyer.
    end if
End Procedure
```

3.4 Auction Phase

As shown in Figure 7, BR who have K_i for the auction could now bid at higher pricing. The participation qualification of BR is confirmed by OAP, whereas SL is in charge of determining the current highest price by comparing legal offers to the current highest price and making a formal announcement.

Step 1. BR chooses a price P_r and the set L, which L is a randomly chosen collection of public keys. Assuming that the kth in L is the public key of BR, BR creates a ring signature as shown below.

First, choose a random number a and calculate,

$$c_{k+1} = h\left(L, P_r, g^a \bmod p\right) \tag{32}$$

Then pick a random number S_i and calculate,

$$c_{i+1} = g^{S_i} y_i^{c_i} \bmod p \tag{33}$$

Calculate S_k using the private key x_k, as a result, the ring forms a closed loop.

$$S_k = a - x_k c_k \bmod q \tag{34}$$

$R = (c_0, \mathrm{S}_0, \mathrm{S}_1, \mathrm{L}\ , \mathrm{S}_{l-1})$ is used as the ring signature. Encrypt $\left(P_r, R, L\right)$ to obtain C_1, and $\left(C_1, K_i^{'}\right)$ to obtain C_2.

$$C_1 = Enc_{pro1}\left(P_r, R, L\right) \tag{35}$$

$$C_2 = Enc_{pro2}\left(F_1, K_i, T_9\right) \tag{36}$$

Afterward, select a random integer t_5 to generate the signature $\left(\theta_{BR_2}, \beta_{BR_2}\right)$. Send $\left(\theta_{BR_2}, \beta_{BR_2}, C_2\right)$ to OAP.

$$\theta_{BR_2} = h\left(C_2, g^{t_5} \bmod p\right) \tag{37}$$

$$\beta_{BR_2} = t_5 + x_k \theta_{BR_2} \bmod q \tag{38}$$

Step 2. OAP first decrypts C_2 before confirming the timestamp's validity.

$$\left(C_1^{'}, K_i^{'}, T_9^{'}\right) = Dec_{pro2}\left(C_2\right) \tag{39}$$

$$Check\left(T_{10} - T_9^{'}\right) < \Delta T \tag{40}$$

If equation (40) is true, then check if $\left(\theta_{BR_2}, \beta_{BR_2}\right)$ is validated.

$$\phi_5 = g^{\beta_{BR_2}} y_k^{\theta_{BR_2}} \bmod p \tag{41}$$

$$\theta_{BR_2} \stackrel{?}{=} h\left(C_2, \phi_5\right) \tag{42}$$

Equation (42) remains true, showing that the OAP accepts the bid proposal. OAP verifies qualification y_k via $K_i^{'}$. If $K_i^{'}$ is bound to y_k, update the ledger to store B_{ij}.

$$B_{ij} = h\left(C_1^{'}, y_k\right) \tag{43}$$

$$M_2 = \left(C_1^{'}, T_{11}\right) \tag{44}$$

Finally, choose a random number t_6 to sign M_2 and send $\left(\theta_{OAP_3}, \beta_{OAP_3}, M_2\right)$ to SL.

$$\theta_{OAP_3} = h\left(M_2, g^{t_6} \bmod p\right) \tag{45}$$

$$\beta_{OAP_3} = t_6 + x_{OAP} \theta_{OAP_3} \bmod q \tag{46}$$

Step 3. SL verifies the validity of the timestamp and decrypts C_1.

$$Check\left(T_{12} - T_{11}^{'}\right) < \Delta T \tag{47}$$

$$(P_r^{'}, R^{'}, L^{'}) = Dec_{pro1}\left(C_1^{'}\right) \tag{48}$$

Then verify the signature $\left(\theta_{OAP_3}, \beta_{OAP_3}\right)$,

$$\phi_6 = g^{\beta_{OAP_3}} y_{OAP}^{\theta_{OAP_3}} \bmod p \tag{49}$$

$$\theta_{OAP_3} \stackrel{?}{=} h\left(M_2, \phi_6\right) \tag{50}$$

OAP has approved the transaction, as shown by the validation of the equation (50) as passed. SL then verifies the ring signature $R^{'}$.

$$e_i = g^{S_i} y_i^{c_i} \bmod p \tag{51}$$

$$c_{i+1} = h\left(L^{'}, P_r^{'}, e_i\right) \tag{52}$$

$$c_0 \stackrel{?}{=} h\left(L^{'}, P_r^{'}, e_{l-1}\right) \tag{53}$$

If equation (53) holds, R is legal. Then call function $calMaxPrice\left(P_r^{'}, R^{'}\right)$, compare $P_r^{'}$ with $CurWinInfo.price$ to get the current winner information.

Algorithm 6 shows the generation of the transaction ring signature, and **Algorithm 7** shows the verification process of the transaction ring signature. **Algorithm 8** allows calculating the current winner.

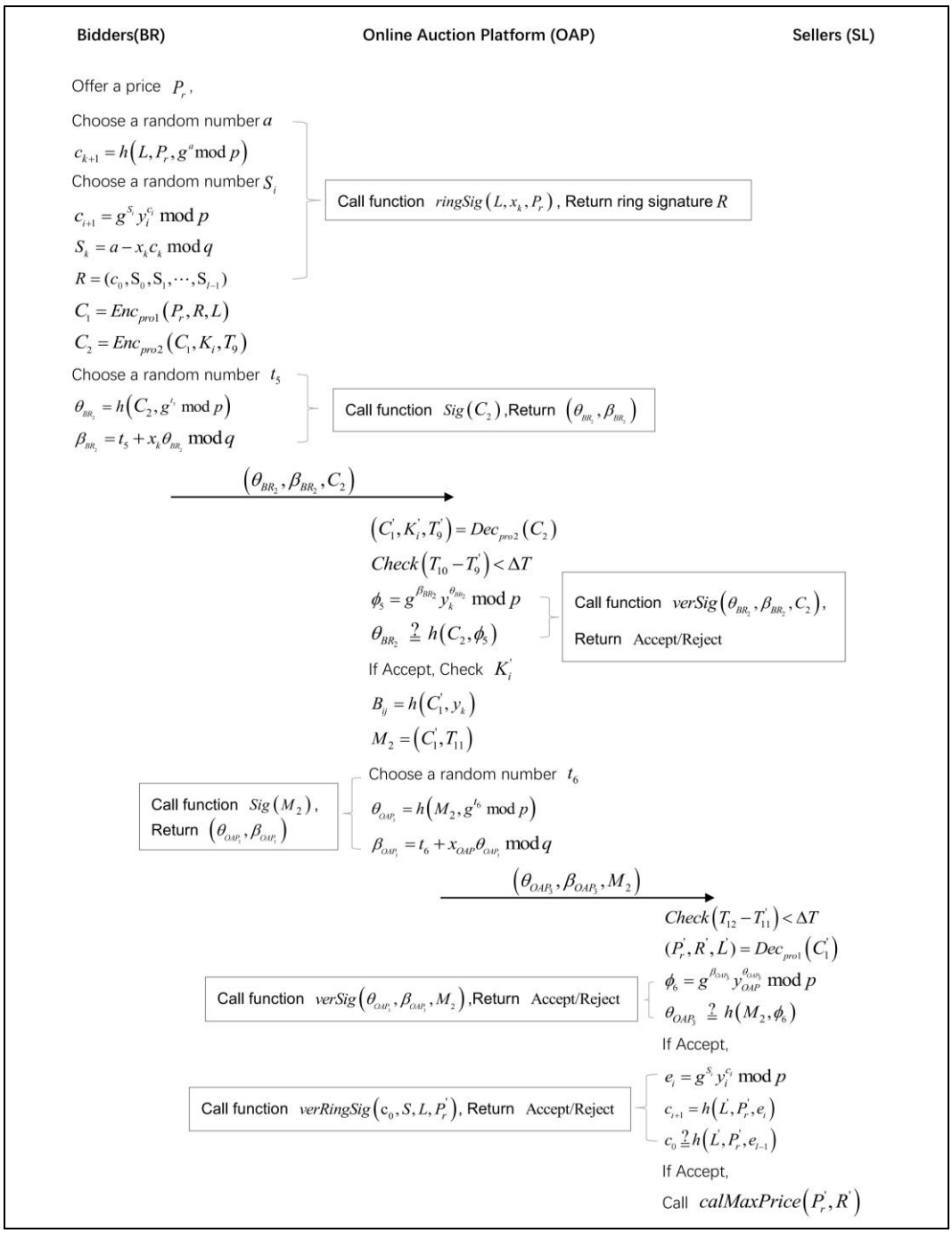

Figure 7. Auction Phase

Algorithm 6. Generate a ring signature.

```
Procedure ringSig (L, _sk, _m)
    Define Q as the number of the ring remember.
    Define char *C[Q] as a one-dimensional array.
    Define int *S[Q] as a one-dimensional array.
    K <- Execute the loop function to find the position of the real signer's public key in the array
L.
    Random Select a;
    C[k+1] <- h(L, _m, g^a mod p);
    for (int i<-k+1; i< Q-1; i++){
        Random choose a number S[i];
            y <- L[i];
            _c <- (g^s) * (y^C[i]) mod p;
            if (i == Q-1) then
                C[0] <- h(L, _m, _c);
            else
                C[i+1] <- h(L, _m, _c);
            end if
    }
    for (int j=0; j<k; j++) {
        Randomly choose a number S[j];
        y <- L[j];
        _c <- (g^b) * (y^C[i]) mod p;
        C[j+1] <- h (L,_m, _c);
    }
    Calculate S[k] <- a - (_sk *C[k]) mod q to make the ring closed.
    Take R <-(C[0], S) as the output ring signature.
End procedure
```

Algorithm 7. Verify the ring signature.

```
Procedure verRingSig (c, S, L, _m)
    Define char *C[Q] as a one-dimensional array.
    Define int *E[Q] as a one-dimensional array.
    Calculate the start point,
    E[0] <- (g ^ S[0]) *(L[0])^c mod p;
    C[1] <- h(L, _m, E[0]);
    for (i=1; i<Q-1; i++){
        y=L[i];
        E[i]=g ^S[i] * y^C[i] mod p;
        if (i==Q-1) then
            C[0] = h(L, _m, E[i]);
        else
            C[i+1] = h(L, _m ,E[i]);
        end if
    }
    if (C[0] == c) then
        The signature is Accepted.
    else
        The signature is Reject.
    end if
End procedure
```

Algorithm 8. Get the current highest bidder.

```
Define CurWinInfo as a global variable.
Function calMaxPrice (_p, _r, _l)
    if (_p >CurWinInfo.price) then
        CurWinInfo.price <- _p;
        CurWinInfo.ringSig <- _r;
        CurWinInfo.L<- _l;
    else
        This auction failed.
    end if
```

3.5 Announce Winner Phase

Following the Auction Phase, OAP publishes the winner's public key based on auction data, as seen in Figure 8.

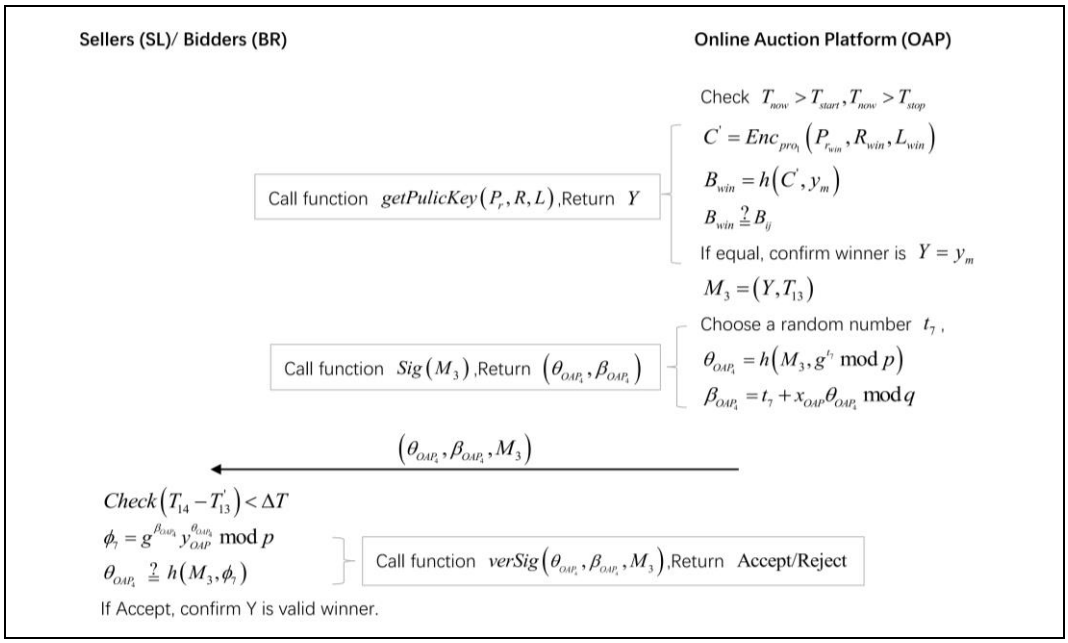

Figure 8. OAP reveals the winner's public key.

Step 1. OAP first verifies the auction deadline to ensure $T_{now} > T_{start}$ and $T_{now} > T_{stop}$. Then compute C' and B_{win}.

$$C' = Enc_{pro_1}\left(P_{r_{win}}, R_{win}, L_{win}\right) \tag{54}$$

$$B_{win} = h\left(C', y_m\right) \tag{55}$$

Next, run a query to the ledger and contrast B_{win} with the record B_{ij} there. Identify the final winning public key Y by getting the B_{ij} one that fulfills the equation (56).

$$B_{win} \stackrel{?}{=} B_{ij} \tag{56}$$

Then, OAP chooses a random number t_7 to sign the information M_3 before sending it to SL and BR.

$$M_3 = \left(Y, T_{13}\right) \tag{57}$$

$$\theta_{OAP_4} = h\left(M_3, g^{t_7} \bmod p\right) \tag{58}$$

$$\beta_{OAP_4} = t_7 + x_{OAP}\theta_{OAP_4} \bmod q \tag{59}$$

Step 2. SL and BR receive M_3 and verify the validity of the timestamp first.

$$Check\left(T_{14} - T_{13}'\right) < \Delta T \tag{60}$$

If the timestamp is valid, then verify the signature $\left(\theta_{OAP_4}, \beta_{OAP_4}\right)$.

$$\phi_7 = g^{\beta_{OAP_4}} y_{OAP}^{\theta_{OAP_4}} \bmod p \tag{61}$$

$$\theta_{OAP_4} \stackrel{?}{=} h\left(M_3, \phi_7\right) \tag{62}$$

The eventual winner is assured to be Y if equation (62) holds. Based on the details of the winning auction, **Algorithm 9** demonstrates how OAP discovers the winner's public key.

Algorithm 9. Get the winner's public key.

```
Procedure getPublicKey (_p, _r, L)
    Let Y= null;
    if (time.now>time.start && time.now >time.end)
        Let C' be the Encrypt (_p, _r, L);
        int len <- the number of elements in the array L;
        for (int i=0; i<len; i++) {
            B[i]=h(C', L[i]);
            Search the ledger,
            if (B[i] is recorded in ledger) then
                Y<-L[i];
                Return Y.
            else
                The auction is not over yet.
            end if
    end if
End Procedure
```

3.6 Dispute Resolution Phase

There are many different forms of disagreements, but they may typically be split into two groups. The first is a disagreement application made by the buyer, while the second is a dispute application initiated by the seller. Through Dispute Scenario 1 and Dispute Scenario 2, we go into great depth about this.

Dispute Scenario 1. When an auction cannot be finished because of a malicious winner who fails to make the final payment within the time given. Now that the seller knows about the buyer's deposit payment DID_i and the winning bid's signature R, they may utilize (AID_i, DID_i, R) to ask the DA for arbitration. The dispute resolution protocol for SL as an applicant is shown in Figure 9. Details of the process are as follows.

Step 1. SL transfers (AID_i, DID_i, R) to the DA for arbitration.

Step 2. After receiving the application, the DA will first confirm the applicant as the seller of AID_i.

If not, the application is invalid. Then, the DA confirms the winner's ring signature R via AID_i and DID_i. Next, check to see if the R provided by SL is consistent R_{win}. If $R = R_{win}$, it means that the ring signature R is valid and SL's application is legitimate. Finally, DA informs the actual signer y_{win} that the balance payment is necessary.

Step 3. If there are no objections, the final payment is made to SL and the final payment record BID_i is sent to OAP after y_{win} getting the notice. Alternatively, if the winner has already made the final payment, he should give OAP the final payment record BID_i immediately.

Step 4. Based on the payment record BID_i that BR provided, DA examines whether the final payment has been made. If it does, the dispute is settled and the request for arbitration is approved. If not, DA informs OAP that BR of y_{win} has broken the regulations.

OAP can penalize BR based on the results of the DA review and the behavior of y_{win}. By using equations (63) and (64) respectively, the OAP has the effect of reducing the user's credit and preventing BR from using the system going forward.

$$UserInfo[credit] = low \tag{63}$$

$$UserInfo[punished] = true \tag{64}$$

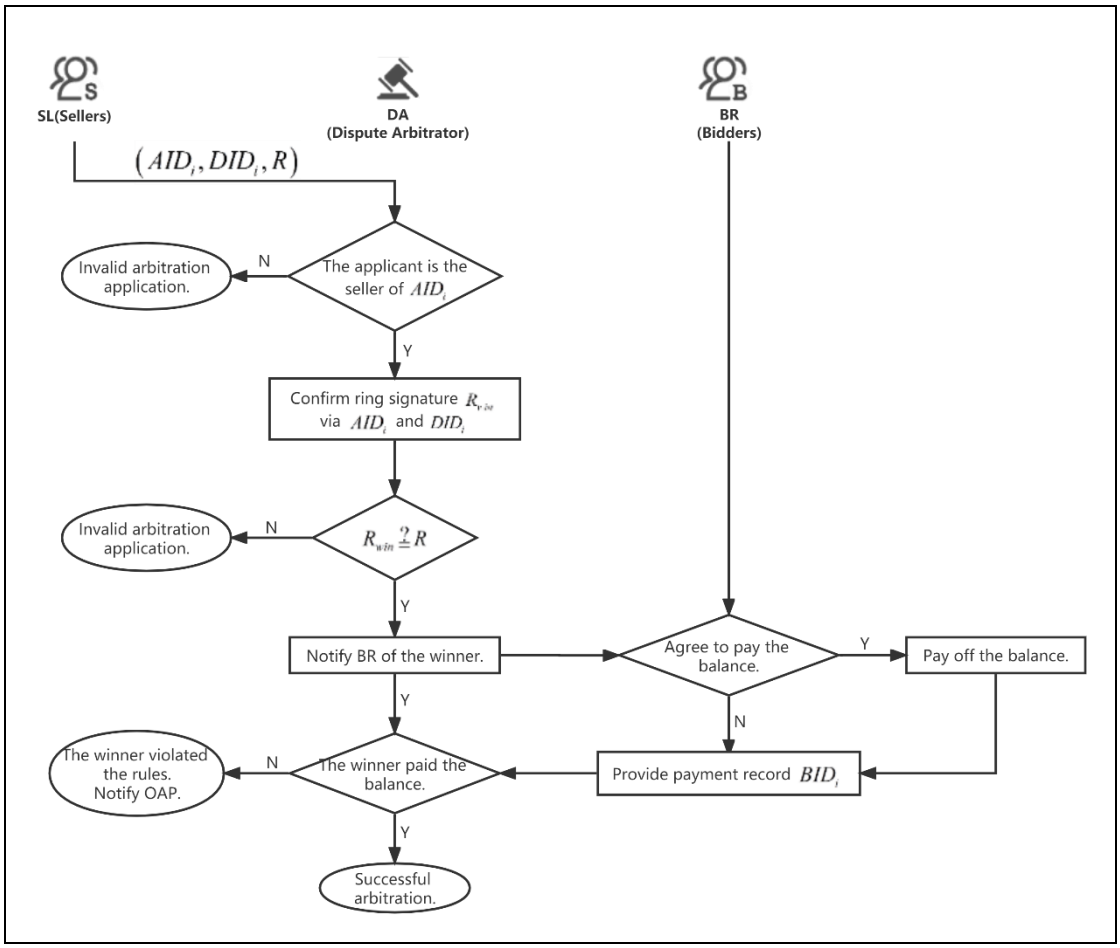

Figure 9. Flow chart of disputes over balance payment.

Dispute Scenario 2. When the winning bidder requests a refund from SL after not receiving the promised auction. Alternatively, BR may request a refund if they get an auction item and discover that it does not match the merchant's description. The buyer can apply to the DA for arbitration by submitting to the DA the auction ID (AID_i), the record of the final payment (BID_i), the ring signature(R) of the bidding transaction, the description of the lots (HV_i), and the results of the third-party appraisal (FID_i). Figure 10 illustrates the dispute handling process of BR as the claimant. The detailed process is as follows.

Step 1. Applicant submits $(AID_i, BID_i, R, HV_i, FID_i)$ to DA.

Step 2. DA first confirms the winner's public key y_{win} and the winner's ring signature R_{win} for auction AID_i . Then determine if the applicant is the winner, if not then the BR application is invalid. If yes, confirm whether the final payment BID_i is part of the auction AID_i and is paid by the applicant. If the applicant is the winner, DA compares the results of the third-party appraisal (FID_i) with the description of the product (HV_i) to determine whether SL is required to return the money. If SL needs to refund money to the applicant, notify SL, otherwise, the dispute is over.

Step 3. If SL agrees to the refund request, it provides the refund, the dispute processing is completed, and the application for arbitration is successful. If SL disagrees, SL needs to provide supporting documents FID_i (such as logistics records, and a certificate from a third-party) to DA.

Step 4. The DA takes additional review based on the supporting papers it has received. There are three chances for SL to present its arguments. If SL refuses to consent to a refund after being asked more than three times, the DA will alert the OAP that SL is breaking the rules. OAP punishes SL for following the results of DA's review and SL's behavior, as illustrated in equations (63) and (64).

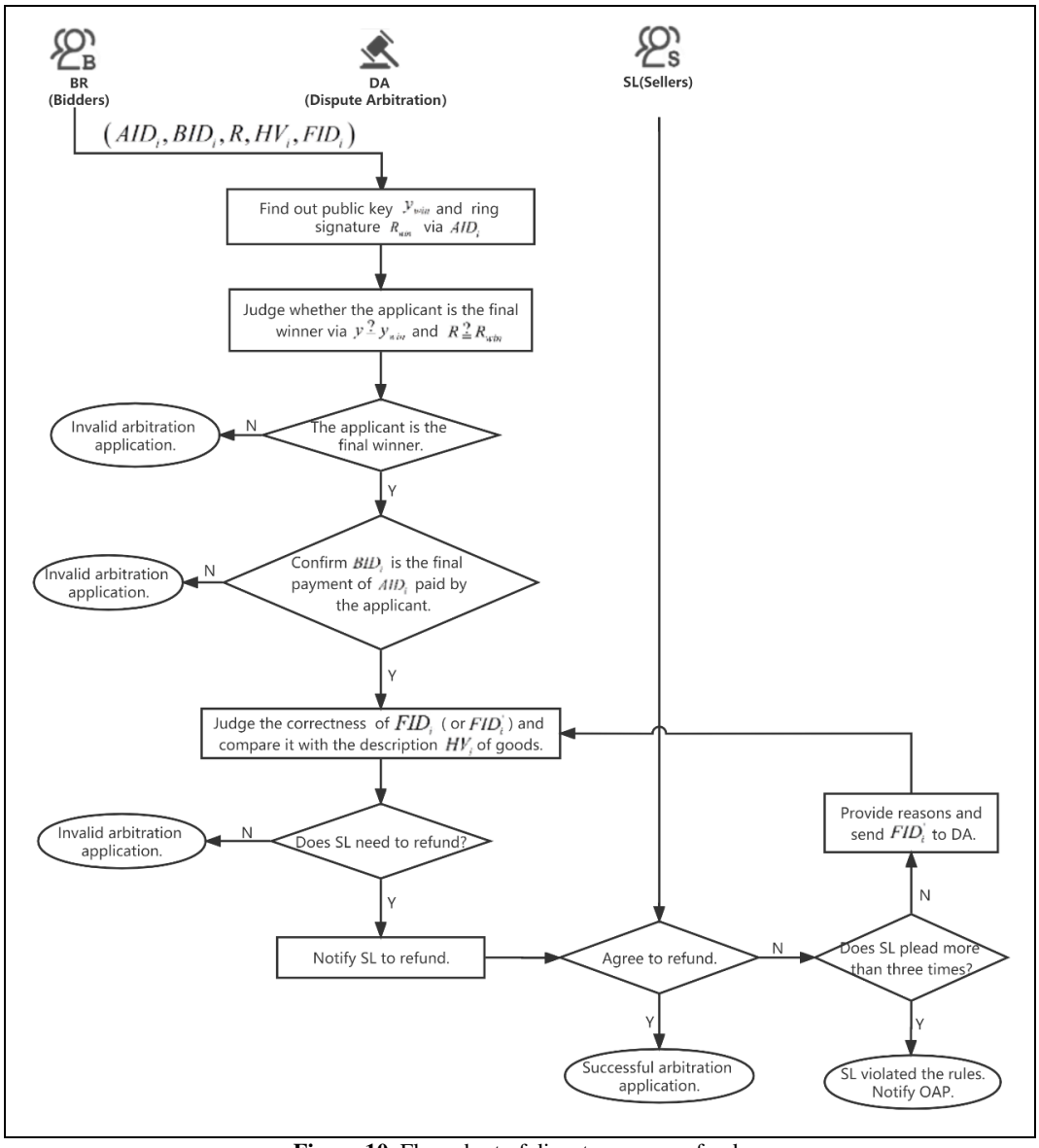

Figure 10. Flow chart of disputes over a refund.

4. Analysis

A system that strikes a balance between many factors and is the outcome of several factors is an appropriate and efficient auction system. Our solution's security performance is based on ring signatures and blockchain technology.

4.1 Data Integrity

A blockchain distributed ledger is used to record the trade data created throughout the bidding process. Every user could notice the changes to the data since the data on the chain is open and transparent. The correctness and dependability of the data are guaranteed by the cryptographic operation and signature, respectively. The recipient can quickly spot it during the verification phase if the data was altered by a hostile party during transmission. Let's take the Auction Phase as an example. When BR engages in the auction, he first encrypts the data to be sent in constructing an encrypted message C_2. The signature $\left(\theta_{BR_2}, \beta_{BR_2}\right)$ is then created using his own private key x. Equations (65), and (66) are used by OAP to check the validity of the signature when it receives a message from BR. The signature $\left(\theta_{BR_2}, \beta_{BR_2}\right)$ is valid and the data received $C_2^{'}$ is trustworthy if equation (66) is true. The OAP then examines the message's accuracy by contrasting the message $C_2^{'}$ it has just received with the message C_2 it has just received from the BR. This implies that when equations (66) and (67) hold simultaneously, the message's integrity is confirmed.

$$\phi_5 = g^{\beta_{BR_2}} y_k^{\theta_{BR_2}} \bmod p \tag{65}$$

$$\theta_{BR_2} \stackrel{?}{=} h\left(C_2, \phi_5\right) \tag{66}$$

$$C_2^{'} \stackrel{?}{=} C_2 \tag{67}$$

4.2 Unforgeability

Firstly, there is very little chance that attacker A will successfully fake a signature. Assume that the probability of attacker A successfully forging a signature is P_a. When attacker A generates a signature by pretending to be an actual signer, this signature must pass verification to be accepted. Equation (68) demonstrates that attacker A may successfully forge a signature that can be validated if he predicts the value t.

$$h\left(m,e\right) = h\left(m, g^s, y^c\right) = h\left(m, g^{t-xc}(\mathrm{g}^{\mathrm{x}})^{\mathrm{c}}\right) = h\left(m, g^t\right) \tag{68}$$

Due to $t \in \left(1,2,\mathrm{L}\ ,q\right)$, we may draw that $P_a = 1/q$. And because of $q \geq 2^{140}$, the chance that attacker A successfully forges a signature by speculating the value t is $P_a \leq 1/2^{140}$. For a message to be acknowledged during the auction, it must be signed with a private key x by the sender and validated by a third party. We take the Auction Phase as an example.

Attacker A, who pretends to be BR to participate in the auction, is only able to produce the signature (θ_A, β_A) using his private key x_A as the probability is $\leq 1/2^{140}$ that he gets the real signer's private key. Furthermore, OAP validates the signature with equations (69), and (70) when the message is received.

$$\phi_5 = g^{\beta_{BR_2}} y_k^{\theta_{BR_2}} \bmod p \tag{69}$$

$$\theta_{BR_2} \stackrel{?}{=} h\left(C_2, \phi_5\right) \tag{70}$$

A faked signature cannot be confirmed since it cannot be matched using equation (70), which shows that the signature is invalid.

Therefore, attacker A cannot participate in the auction by forging a signature.

4.3 Non-repudiation

Using the Schnorr digital signature, this approach ensures non-repudiation of the sender's identity. There is a negligible possibility ($\leq 1/2^{140}$) that the real signer's private key is being revealed, according to the proof of section 4.2. Table 2 shows the signature and verification signature for each stage based on this. Every step of the data transmission process has to be signed with the sender's private key and verified by the recipient using the sender's public key. As a result, when the verification equations are true, the signature is genuine and the signer cannot deny it.

Table 2. Non-repudiation of the proposed Scheme.

Phase \ Item	Proof	Issuer	Holder	Verification Equation
Pre-auction Phase	$\left(\theta_{SL_2}, \beta_{SL_2}\right)$	*SL*	*OAP*	$\phi_1 = g^{\beta_{SL_1}} y_{SL}^{\theta_{SL_1}} \bmod p\ ;\ \theta_{SL_1} \stackrel{?}{=} h\left(C_{\mathrm{lot}}, \phi_1\right)$
	$\left(\theta_{OAP_1}, \beta_{OAP_1}\right)$	*OAP*	*SL*	$\phi_2 = g^{\beta_{OAP_1}} y_{OAP}^{\theta_{OAP_1}} \bmod p\ ;\ \theta_{OAP_1} \stackrel{?}{=} h\left(C_{res_1}, \phi_2\right)$
	$\left(\theta_{BR_1}, \beta_{BR_1}\right)$	*BR*	*OAP*	$\phi_3 = g^{\beta_{BR_1}} y_{BR}^{\theta_{BR_1}} \bmod p\ ;\ \theta_{BR_1} \stackrel{?}{=} h\left(C_{BR}, \phi_3\right)$
	$\left(\theta_{OAP_2}, \beta_{OAP_2}\right)$	*OAP*	*BR*	$\phi_4 = g^{\beta_{OAP_2}} y_{OAP}^{\theta_{OAP_2}} \bmod p\ ;\ \theta_{OAP_2} \stackrel{?}{=} h\left(C_{res_2}, \phi_4\right)$
Auction Phase	$\left(\theta_{BR_2}, \beta_{BR_2}\right)$	*BR*	*OAP*	$\phi_5 = g^{\beta_{BR_2}} y_k^{\theta_{BR_2}} \bmod p\ ;\ \theta_{BR_2} \stackrel{?}{=} h\left(C_2, \phi_5\right)$
	$\left(\theta_{OAP_3}, \beta_{OAP_3}\right)$	*OAP*	*SL*	$\phi_6 = g^{\beta_{OAP_3}} y_{OAP}^{\theta_{OAP_3}} \bmod p\ ;\ \theta_{OAP_3} \stackrel{?}{=} h\left(M_2, \phi_6\right)$
Announce Winner Phase	$\left(\theta_{OAP_4}, \beta_{OAP_4}\right)$	*OAP*	*SL or BR*	$\phi_7 = g^{\beta_{OAP_4}} y_{OAP}^{\theta_{OAP_4}} \bmod p\ ;\ \theta_{OAP_4} \stackrel{?}{=} h\left(M_3, \phi_7\right)$

4.4 Traceability

By storing all transaction data on the blockchain, this system ensures that the data is secure and that the transaction data can be tracked. During the Auction Phase, each incremental bid needs to be approved by the OAP. For the legitimate bid information $C_1^{'}$ (containing bid price P_r, ring

signature R, and public key set L) and bidder's public key y_k, OAP computes a hash value and stores it in the ledger.

$$B_{ij} = h\left(C_1^{'}, y_k\right) \tag{71}$$

At the end of the bidding, OAP calculates the B_{win} by equations (72) and (73). The winner y_m is then determined by comparing the records B_{ij} that are equal B_{win}, as illustrated in (74).

$$C^{'} = Enc_{pro_1}\left(CurWinInfo.price, CurWinInfo.ringSig, CurWinInfo.L\right) \tag{72}$$

$$B_{win} = h\left(C^{'}, y_m\right) \tag{73}$$

$$B_{win} \stackrel{?}{=} B_{ij} \tag{74}$$

Thus, we can track the winning bidder once the auction is closed.

4.5 Verifiability

Each bid transaction $\left(P_r, R, L\right)$ will be recorded in the blockchain ledger, and when the ledger is updated, everyone will be aware of the update. In the bidding process, after the data $\left(P_r, R, L\right)$ is uploaded, other people can easily verify the validity of R and know the specifics P_r by using equations (51), (52), and (53). When the auction ends, the OAP will announce the final winner's public key, and the other participants can verify whether L is contained y_{win} by comparing it with the public key y_i in L. In addition, others can calculate the winner's information B_{win} and compare it with previous records in the ledger to see if the winner is legitimate. If B_{win} is not questioned, then y_{win} is not the declared winner, meaning that the winner is invalid.

$$C^{'} = Enc_{pro1}\left(P_{r_{win}}, R_{win}, L_{win}\right) \tag{75}$$

$$C_{win} = h\left(C^{'}, y_{win}\right) \tag{76}$$

Thus, it is said that in our program, anyone can verify the auction results.

4.6 Easy revocation

Unlike the method [5], their approach is vulnerable to attacks and cannot appropriately cancel the user's rights in their system. Our scheme makes it easy to manage the rights of the user in the system. Depending on the seriousness of the malicious person's violation, OAP may apply sanctions such as a decrease in credit level or a ban on the malicious person's ongoing use of the system. Also, the bidding transactions initiated by violators will be deemed invalid.

Scenario: The user U_c is the winner of an auction, but is late in paying the final payment to SL. Following the SL appeal, the DA decides that the consumer must make the final payment on time. However, after receiving the judgment, the U_c still refused to pay the final payment without legitimate reason, and the OAP confirmed that U_c seriously damaged the interests of the SL.

Analysis: Because of the severity of the violation, the OAP will penalize the user by reducing their credit level and disabling to use of the system. First, the OAP reduces the user's credit score.

$$UserInfo[credit] = low \tag{77}$$

Second, OAP revokes the bid and restricts U_c from continuing to use the system.

$$UserInfo[punished] = true \tag{78}$$

Even if U_c reapplies for a new account after being deactivated, he or she cannot register for a new account to utilize the auction system since his or her ID already exists in the registration list.

4.7 Anonymity

First, users use the system using a pseudonym (public key Y), which protects their privacy to a certain extent. Second, the use of ring signatures in this scheme improves the privacy of the bidders. The public key of the real bidder is hidden in a set of public keys L. Except for OAP, the odds that a participant guesses the probability of the real bidder's public key Y_{BR} is $1/l$ (l is the number of public keys in the public key set L). The malicious person can only determine that the

bidder's public key is in the set L, but cannot determine which one is the actual sender. By preventing a hostile party from tracing the transaction details of a fixed public key address, they are unable to determine which auction products the public key holder has bid on and what his preferences are. This maximizes the bidder's online privacy. Last but not least, the identity of the public key holder cannot be revealed by anybody other than the OAP, and it will not be.

Therefore, the user is anonymous and the user's privacy is guaranteed.

4.8 Fairness

The fairness of online auction transactions is influenced by many factors and is a comprehensive indicator. First, in our approach, information regarding the most recent auction status is distributed synchronously and consistently to all participants. Second, we lessen the chances that SL and BR will rig the bidding. The real bidder of each transaction is confusing to SL because of the ring signature algorithm, hence SL is unbiased in confirming the ring signature to assure a greater reward. Additionally, due to the transparency and traceability provided by a blockchain, the bidding process can be monitored by the public to encourage fairness. Finally, to protect the rights and interests of lawful users, we settle disputes in auctions using a fair and efficient dispute resolution procedure that takes into account all the necessary details.

Therefore, our auction agreement is a fair auction system.

4.9 Resist Known Attacks

(1) DoS Attacks

DoS attacks would prevent regular users from accessing services by using system resources and network bandwidth, or by exploiting flaws in the system to paralyze regular services in regular systems. The decentralized nature of the blockchain allows the blockchain to continue to operate and verify transactions even if one node fails and the other nodes are not affected, and the whole system can continue to operate normally. When the failed nodes resume work, they resynchronize and catch up with the latest data provided by the unaffected nodes. We use a blockchain distributed ledger to store data rather than a central server, and this decentralized nature makes the cost of an attack enormous, making it difficult for a potential attacker to execute an attack operation.

(2) Sybil Attacks[34]

A Sybil attack is an effort to acquire network control, refuse replies, and interfere with requests by disguising a node as numerous nodes and broadcasting these multiple disguised nodes (Sybil nodes) to the whole P2P network. The way to implement the witch attack is to spoof the network ID. Malicious bidders may tamper with the bidding process to increase their profit by creating various identities and claiming to be multiple users to participate in the auction. A user identity access mechanism is used in our scheme, and each joining node needs to register an account with OAP by providing an identity ID to use the system. When OAP distributes a public-private key for a new user, it first checks whether the identity ID submitted by the user already exists in the system and does not distribute a new public-private key for it if it does. In other words, an ID can only apply for a seller's public key y_{seller} as "seller" or a buyer's public key y_{bidder} as "bidder". Consequently, a malicious individual cannot create various identities to pose as different users to engage in the auction. Furthermore, in the blockchain context, nodes must execute a large number of calculations to confirm their authenticity, making Sybil attacks prohibitively expensive and useless. As a result, our case is immune to Sybil's assaults.

(3) Replay Attacks

When a replay attack is launched, a legal data transfer will be continually and maliciously repeated to the receiver. We prevent replay attacks by adding timestamps T_i at each stage in combination with signatures (the purpose of signatures is to prevent session hijacking and timestamps from being modified). The receiver confirms the validity of the timestamp and verifies the signature upon receipt of the message. Taking Auction Phase as an example, when BR needs to transmit data to OAP, it adds a timestamp T_9 to the encrypted message.

$$C_2 = Enc_{pro2}\left(C_1, K_i, T_9\right) \tag{79}$$

When the OAP receives the message, it verifies that the timestamp is valid by equation (80).

$$Check\left(T_{10} - T_9^{'}\right) < \Delta T \tag{80}$$

If equation (80) does not hold, it means that the timestamp is invalid and a replay attack will be identified as occurring. Suppose a replay attack is launched by a malicious person A. The A hijacks C_2 and modifies the timestamp T_9 to T_{9-1}. When A sends the same message (C_1, K_i) to OAP, OAP will first check the validity of the timestamp T_{9-1}. The timestamp is deemed incorrect and a replay attack takes place if the difference between the current time and T_{9-1} does not meet the requirement.

5. Discussion

5.1 Computation Cost

At each stage, participants are required to sign the transmitted data, encrypt and decrypt them by using symmetric encryption and decryption algorithms. These computational costs are shown in Table 3, in which we compare the effective computational overhead at each stage.

Table 3. Calculate computation cost at each phase.

Role / Phase	Role A	Role B	Role C
Pre-auction Phase	Sellers $2T_{asc}+2T_h+T_{add}+$ $T_{sub}+2T_{mul}+3T_{\exp}$	Online Auction System $2T_{asc}+2T_h+T_{add}+$ $T_{sub}+2T_{mul}+3T_{\exp}$	
	Bidders $2T_{asc}+(l+1)T_h+T_{add}+$ $T_{sub}+2T_{mul}+(3l+1)T_{\exp}$	Online Auction System $2T_{asc}+2T_h+T_{add}+$ $T_{sub}+2T_{mul}+3T_{\exp}$	
Auction Phase	Bidders $2T_{asc}+(l+1)T_h+T_{add}$ $+T_{sub}+3T_{mul}+(l+2)T_{\exp}$	Online Auction System $T_{asc}+3T_h+T_{add}+$ $T_{sub}+2T_{mul}+3T_{\exp}$	Sellers $T_{asc}+(l+2)T_h+T_{sub}$ $+2T_{mul}+2(l+1)T_{\exp}$
Announce Winner Phase	Sellers/ Bidders $T_h+T_{sub}+T_{mul}+2T_{\exp}$	Online Auction System $T_{asc}+(l+1)T_h+T_{add}+$ $T_{mul}+T_{\exp}$	

Note: T_{asc}: time complexity of asymmetrical encryption/decryption; T_h: time complexity of a hash operation; T_H: time complexity of a Hash operation; T_{add}: time complexity of an additional operation; T_{sub}: time complexity of a subtraction operation; T_{mul}: time complexity of a multiplication operation; T_{div}: time complexity of a division operation; $T_{\exp}$: time complexity of an exponentiation operation; l: number of public keys in set *L*.

5.2 Communication Cost

Table 4 provides an analysis of the system's communication effectiveness. We will analyze the communication costs under 3G, 4G, and 5G individually due to the various communication settings. The top 3G, 4G, and 5G transmission speeds are 6 Mbps, 100 Mbps, and 20 Gbps respectively.

In our scheme, the Auction Phase is where users interact with the system most frequently, and the communication cost is something we should consider, for instance. When BR submits a price, the data C_1 to be transferred (including bid price P_r, ring signature R, and public key set L) is $[128+(160+160*l)+512*l]=288+672*l$ bits. The data C_2 to be transferred (including data C_1, participation credentials K_i, and timestamps T_9) is $[(288+672*l)+128+80]=672*l+496$ bits. In the process of transferring data from BR to OAP, the transferred data consists of data C_2

and a signature (θ, β), and the data size is $[(672*l+496)+212]=(672*l+708)$ bits. When OAP transferred data to SL, the transferred data consists of data C_1, a timestamp T_{11}, and a signature (θ, β). The data size is $[(288+672*l)+80+212]=(672*l+580)$ bits.

Thus, the total transferred data size is $(1344*l+1288)$ bits. It can be seen that in a 3G environment, the process takes time $(224*l+214.67)$ us. Taking $(13.44*l+12.88)$ us in a 4G environment and $(0.068*l+0.065)$ us in 5G environment. Assuming that the bidder selects 20 public keys (including its public key) to form a ring signature, the total size of the data transferred in this process is 28296 bits. In a 3G environment, the time consumption is 4716 us, in a 4G environment the time consumption is 282.96 us, while in a 5G environment it only takes 1.431 us.

Table 4. Communication cost at each phase.

Item / Phase	Message Length (bits)	3G (6 Mbps)	4G (100 Mbps)	5G (20 Gbps)
Pre-auction Phase	2320	386.67us	23.2 us	0.116 us
Auction Phase	$1344*l+1288$	$(224*l+214.67)us$	$(13.44*l+12.88)us$	$(0.068*l+0.065)us$
Announce Winner Phase	804	134 us	8.04 us	0.041 us

5.3 Performance Analysis

In this section, we perform an experimental evaluation of the proposed scheme. Caliper [35] is a blockchain performance testing framework that supports multiple blockchain platforms such as Hyperledger Fabric, Ethereum, and FISCO BCOS. We deployed the test scenario on a server with an 11th Gen Intel(R) Core (TM) i5-11400F @ 2.60 GHz 2.59 GHz CPU and 2GB RAM. We are using Fabric Docker Image version 2.2.0 and Go version 1.13.12. The physical machine OS (Operating System) is Ubuntu 18.04.6 LTS.

We take two smart contracts from the Auction Phase for analysis and use throughput and transaction latency as the main performance metrics for benchmarking. The performance of blockchain applications is affected by many complex or unstable factors and is usually evaluated in terms of both throughput and latency. Throughput, expressed in TPS (Transaction Per Second), is the rate at which transactions are added to the ledger. It is a crucial indicator of the system's processing power. Latency is the amount of time between when an application sends a transaction proposal and when the transaction is committed to the ledger. This is the first thing that users care about when using blockchain applications. We examine the data in our test scenario with the max latency.

Figure 11 shows how throughput changes as the number of transactions increases when the block size and sending rate are fixed. As you can see from the histogram, the TPS has been between 200 and 300 during the test, and it is steadily and slowly increasing. For the contract "*SubmitBidPrice*", the TPS has a minimum value of 214.1 when the transaction volume is set to 500 and reaches a maximum of 268.3 when the transaction volume is set to 5000. For the contract "*UpdateWinnerInfo*", the TPS has a minimum value of 212.7 when the volume is set to 500 and reaches a maximum of 287.4 when the volume is set to 5000. In addition, Figure 12 shows how the max latency varies as the number of transactions increases. As a whole, the latency varies between 0.06s and 0.17s as the number of transactions increases, with an overall upward trend. When the transaction volume is set to 5000, the max latency of "*SubmitBidPrice*" and "*UpdateWinnerInfo*" peaks at 0.13s and 0.17s, respectively.

Combining the data in Figure 11 and Figure 12 and the current usage of blockchain applications, the system performance is passable. However, we should also realize that we can start from several aspects to improve the system's performance. Among them, the mode of multi-chain parallel computing can significantly improve the TPS of the blockchain system, and this is also the direction of our future research.

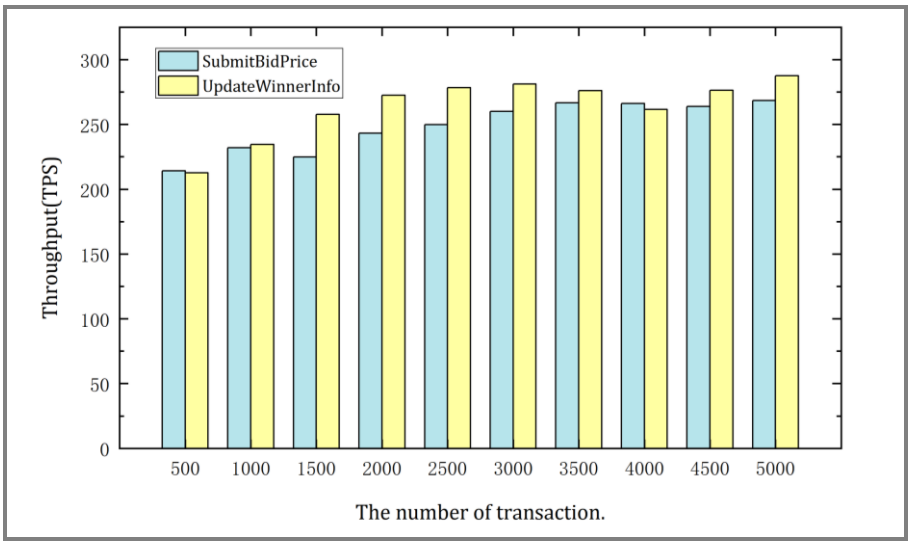

Figure 11. The throughput at different transaction volumes.

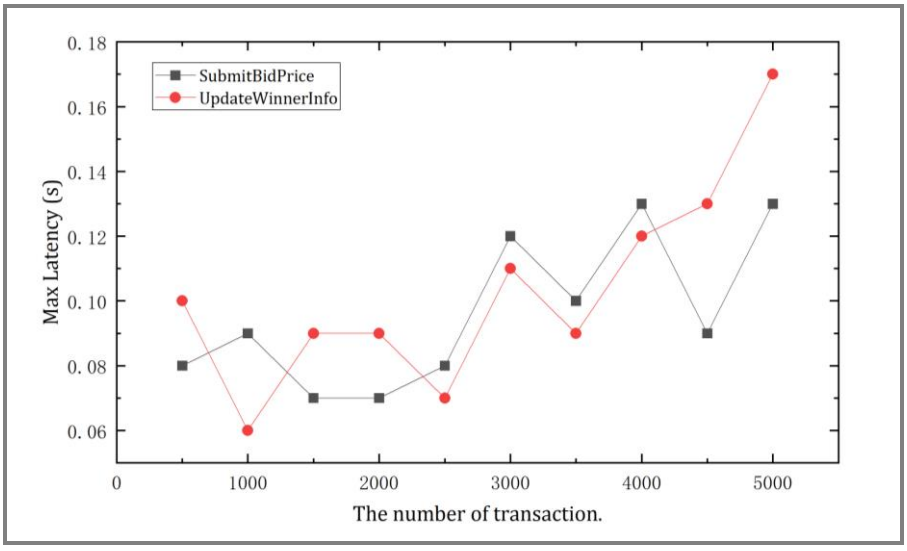

Figure 12. The max latency at different transaction volumes.

Table 5. Compare with other schemes.

Feature \ Scheme		[10]	[5]	[14]	[15]	[6]	[16]	[7]	Ours
Data Security	Transparent	W	W	M	M	M	M	M	R
	Data Integrity	W	W	M	M	M	M	M	R
	Traceability	W	W	M	R	M	M	M	R
Unforgeability		W	W	M	R	M	M	M	R
Non-repudiation		W	W	M	R	M	M	M	R
Traceability		W	W	W	M	R	M	M	R
Easy revocation		W	R	W	M	R	M	M	R
Anonymity		R	W	W	M	W	W	R	R
Fairness		W	W	W	W	W	M	M	R
Dispute resolution plan		Y	Y	N	N	N	N	N	Y

W: weak level; M: medium level; R: robust level.
Y: Yes; N: Not

5.4 Compare with other schemes

Popular systems (such as [6, 14, 16]) lack transactional privacy and pay insufficient attention to user privacy, as we discussed in section 1.2. In our solution, we protect the user's privacy by enhancing the anonymity of the user through ring signatures. Additionally, the majority of the systems (such as [7, 15]) lack a clear dispute management scheme. To address this shortcoming and strengthen the auction agreement, we propose a workable dispute handling technique. Furthermore, our scheme makes use of decentralized blockchain technology to make the auction process transparent, as a lack of transparency in the transaction process (e.g., [5, 10]) might undermine the fairness of online auctions. In Table 5, we contrast our subject with various previous auction cases.

6. Conclusions

Online auctions have a promising future and are an important part of the global economy. A fair online auction environment can enhance people's trust in online auctions and increase their participation in online auctions. In this paper, we propose an anonymous English bidding protocol based on blockchain and ring signatures, detailing how to improve the privacy and fairness of online auctions. We demonstrate different stages of data integrity, unforgeability, and non-reputation, and illustrate the reasons why our protocol is resistant to DoS attacks, replay attacks, and Sybil attacks. Through scenario analysis, the protocol's traceability and ease of revocation are shown, along with how it promotes anonymity and fairness. We also discuss the computation cost at different stages and the communication cost in different network environments, which are reasonable and acceptable.

Compared to other programs, our program has the following three features.

(1) A decentralized online auction system is built using blockchain technology, which provides a secure and transparent online bidding environment, ensuring the transparency of the auction transaction process and that the transaction process is supervisable.
(2) In terms of users' privacy, the proposed ring signature-based anonymous auction protocol enhances user anonymity and ensures user privacy during the transaction, so that users do not have to worry about behavioral data being used by those with an interest.
(3) In terms of disputes, unlike most of the previous research proposals that did not clarify how these disputes would be handled, we propose a clear dispute handling scheme that enhances the fairness of the auction. When interests are compromised, both the grantor and the bidder can obtain a fair result through arbitration.

Author Contributions

The authors' contributions are summarized below. Conceptualization, Z.Y. and C.-L. C.; methodology, Z.Y., Y.-Y. D and C.-L. C.; validation, W.-J.T., W.W. and H.S.; investigation, C.-L.C. and Y.-Y.D.; data analysis, W.-J.T., W.W. and H.S.; writing—original draft preparation, Z.Y. and C.-L. C.; writing—review and editing, W.-J.T., Y.-Y.D. and H.S.; supervision, C.-L.C. and W.W. All authors have read and agreed to the published version of the manuscript.

Funding

This work was supported in part by the Ministry of Science and Technology in Taiwan (No. MOST 111-2218-E-305-001-MBK and MOST 110-2410-H-324-004-MY2), the Natural Science Foundation of Fujian Province of China (No. 2018J01572) , the Science and Technology Project of Jilin Provincial Department of Education (JJKH20210457KJ), Jilin Province Science and Technology Development Plan Project (20220508038RC), Undergraduate Training Programs for Innovation and Entrepreneurship Project of Jilin Province (J202210203JSJ02) and CERNET Innovation Project (NGII20180315), the National Natural Science Foundation for Young Scientists of China (Grant No. 51808474).

Institutional Review Board Statement

This study is only based on theoretical basic research. It is not involving humans.

Informed Consent Statement

This study is only based on theoretical basic research. It is not involving humans.

Data Availability Statement

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest
The authors declare no conflict of interest.

Appendix

(g, p, q)	:System Parameters. p and q are large prime numbers,
(y_U, x_U)	: The public key y and private keys x of U .
ID_U	: The real ID of U .
$Role_U$	: The role U of the system.
$Enc_{phase}(\ ) / Dec_{phase}(\ )$	: Symmetric encryption and decryption functions in each phase.
$(\theta_{U_i}, \beta_{U_i})$	: Schnorr signatures are generated by the user U at different stages.
$h(\ )$	: One-way hash function.
HV_i	: The hash value returned by IPFS for auction i.
f_{cre}	: Credit requirements for bidders from sellers.
f_{dep}	: Deposit requirements for bidders from sellers.
AID_i	: Auction ID of lot i.
DID_i	: ID for deposit transaction record.
K_i	: Participating credentials for bidder BR.
L	: Public key set (with the public key of the real signer).
l	: Length of the public key set L .
P_r	: The price offered by the bidder.
t_i	: Random parameters are used in the signing process.
R	: Ring signature created by the user.
M_x	: Unencrypted transmission information.
C_x	: Encrypted message.
T_i	: Timestamps.
BID_i	: Balance payment transaction ID.
FID_i	: File ID.
RID_i	: Refund transaction ID.

References

1. Global Auction Sales Soared to a Record $12.6 Billion in 2021, Access available: https://www.barrons.com/articles/global-auction-sales-soared-to-a-record-12-6-billion-in-2021-01641328947 , Jan. 4, 2022.
2. Online Auction Market: 8.07% Y-O-Y Growth Rate in 2022 | by Product and Geography - Forecast and Analysis 2022-2026, Access available: https://www.prnewswire.com/news-releases/online-auction-market-8-07-y-o-y-growth-rate-in-2022--by-product-and-geography---forecast-and-analysis-2022-2026--301549132.html , May. 18, 2022.
3. It's a crime to use Google Analytics, watchdog tells Italian website, Access available: https://www.theregister.com/2022/06/24/italy_google_analytics/ , Jun. 24, 2022.
4. Italian data protection authority warns against the use of Google Analytics, Access available: https://www.computing.co.uk/news/4051808/italian-protection-authority-warns-google-analytics, June.24, 2022.
5. Chang C C, Cheng T F, Chen W Y. A novel electronic english auction system with a secure on-shelf mechanism[J]. IEEE transactions on information forensics and security, 2013, 8(4): 657-668.
6. Lee J S, Chew C J, Chen Y C, et al. Preserving liberty and fairness in combinatorial double auction games based on blockchain[J]. IEEE Systems Journal, 2020, 15(3): 3517-3527.
7. Huang K, Mu Y, Rezaeibagha F, et al. BA2P: Bidirectional and Anonymous Auction Protocol with Dispute-Freeness[J]. Security and Communication Networks, 2021, 2021.
8. Lee B, Kim K, Ma J. Efficient public auction with one-time registration and public verifiability[C]//International Conference on Cryptology in India. Springer, Berlin, Heidelberg, 2001: 162-174. pp 162-174

9. Chen T S. An English auction scheme in the online transaction environment[J]. Computers & Security, 2004, 23(5): 389-399.
10. Xiong H, Chen Z, Li F. Bidder-anonymous English auction protocol based on revocable ring signature[J]. Expert Systems with Applications, 2012, 39(8): 7062-7066.
11. Chang C C, Chang Y F. Efficient anonymous auction protocols with freewheeling bids[J]. Computers & Security, 2003, 22(8): 728-734.
12. Jiang R, Pan L, Li J H. An improvement on efficient anonymous auction protocols[J]. Computers & Security, 2005, 24(2): 169-174.
13. Romero Ugarte, José Luis, Distributed Ledger Technology (DLT): Introduction (October 16, 2018). Banco de Espana Article 19/18, Available at SSRN: https://ssrn.com/abstract=3269731
14. Braghin, C., Cimato, S., Damiani, E., Baronchelli, M. (2020). Designing Smart-Contract Based Auctions. In: Yang, CN., Peng, SL., Jain, L. (eds) Security with Intelligent Computing and Big-data Services. SICBS 2018. Advances in Intelligent Systems and Computing, vol 895. Springer, Cham.
15. Enkhtaivan B, Takenouchi T, Sako K. A fair anonymous auction scheme utilizing trusted hardware and blockchain[C]//2019 17th International Conference on Privacy, Security and Trust (PST). IEEE, 2019: 1-5.
16. Qusa H, Tarazi J, Akre V. Secure e-auction system using blockchain: UAE case study[C]//2020 Advances in Science and Engineering Technology International Conferences (ASET). IEEE, 2020: 1-5.
17. Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014, November). Deanonymisation of clients in Bitcoin P2P network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 15-29).
18. Fan L, Xu C X, Li J H. Deniable authentication protocol based on Deffie-Hellman algorithm[J]. Electronics letters, 2002, 38(14): 1.
19. Zheng Z, Xie S, Dai H, et al. An overview of blockchain technology: Architecture, consensus, and future trends[C]//2017 IEEE international congress on big data (BigData congress). Ieee, 2017: 557-564.
20. Golosova J, Romanovs A. The advantages and disadvantages of the blockchain technology[C]//2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE). IEEE, 2018: 1-6.
21. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
22. D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170
23. M. Pors, "Understanding the IPFS White Paper part 2", https://decentralized.blog/understanding-the-ipfs-white-paper-part-2.html, last accessed 2018/3/18.
24. Platform Inter Planetary File System. https://ipfs.io/.
25. Doan T V, Bajpai V, Psaras Y, et al. Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Directions[J]. arXiv preprint arXiv:2202.06315, 2022.
26. Schnorr C P. Efficient identification and signatures for smart cards[C]//Conference on the Theory and Application of Cryptology. Springer, New York, NY, 1989: 239-252.
27. Maxwell G, Poelstra A, Seurin Y, et al. Simple Schnorr multi-signatures with applications to Bitcoin[J]. Designs, Codes and Cryptography, 2019, 87(9): 2139-2164.
28. Nick J, Ruffing T, Seurin Y. MuSig2: simple two-round Schnorr multi-signatures[C]//Annual International Cryptology Conference. Springer, Cham, 2021: 189-221.
29. Schnorr C P. Efficient signature generation by smart cards[J]. Journal of cryptology, 1991, 4(3): 161-174.
30. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M.Voelker, and S. Savage,"A fistful of bitcoins: Characterizing payments among men with no names," in Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13), New York, NY, USA,2013.
31. Barceló, Jaume. "User Privacy in the Public Bitcoin Blockchain." (2014).
32. Rivest R L, Shamir A, Tauman Y. How to leak a secret[C]//International conference on the theory and application of cryptology and information security. Springer, Berlin, Heidelberg, 2001:552-565.
33. Abe M, Ohkubo M, Suzuki K. 1-out-of-n signatures from a variety of keys[C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2002: 415-432.
34. Douceur J R. The sybil attack[C]//International workshop on peer-to peer systems. Springer, Berlin, Heidelberg, 2002: 251-260.
35. Hyperledger Caliper, Access available: https://hyperledger.github.io/caliper/, Sept.1, 2022.