Hindawi
Security and Communication Networks
Volume 2021, Article ID 5523394, 10 pages
https://doi.org/10.1155/2021/5523394

Research Article

A Blockchain-Based Sealed-Bid e-Auction Scheme with Smart Contract and Zero-Knowledge Proof

Honglei Li and Weilian Xue

School of Government, Liaoning Normal University, Dalian, China

Correspondence should be addressed to Weilian Xue; xueweilian@lnnu.edu.cn

Received 22 February 2021; Revised 30 March 2021; Accepted 11 May 2021; Published 19 May 2021

Academic Editor: Leandros Maglaras

e-Auction improves the efficiency of bid transaction. However, the protection of bidders' privacy, transaction fairness and verifiability, transaction data security, high cost of third-party auction center, and other issues have attracted more attention. According to the transaction process and basic principles of the sealed auction, we explored the problems existing in the current sealed-bid e-auction schemes. Based on the blockchain technology, we proposed a sealed-bid e-auction scheme with smart contract technology, Bulletproofs zero-knowledge proof protocols, and Pedersen commitment algorithm. The proposed scheme constructed an auction mechanism without the third-party auctioneer so as to restrict the behaviors of auction parties for the sake of auction security, reliability, fairness, and privacy protection. Compared with the related sealed e-auction schemes based on blockchain technologies in six metrics, we conducted the experiment to show that the proposed scheme protected the bid information from leakage well and successfully verified the winning bid price and the related bidder by all transaction participants without the third-party auctioneer.

1. Introduction

Auction is a common and traditional way to sell goods that are not easy to value. In the transaction, there is a serious information asymmetry between the seller and the buyers. Buyers usually have a strong incentive to hold down prices. Because the seller does not know the important information of the buyer's valuation, the one-turn pricing transaction cannot guarantee the effective allocation of scarce resources. That is, it cannot guarantee the buyer who is considered to be the most valuable owner of the goods. Auction with the reasonable market trading rules makes the full use of the competition between buyers to achieve the effective allocation of resources and other objectives. Since auction plays an important role in resource allocation, many researchers have conducted studies on the improvement of the mechanism of auction. For example, William Vickrey was awarded the Nobel Economics Prize (1996) for his auction theory. Paul Milgrom and Robert Wilson won the Nobel Economics Prize (2020) for their improvements to auction theory and inventions of new auction formats.

In different markets, traditional auctions are divided into sealed-bid auctions and open-bid auctions according to whether the auction price is open or not. In the sealed-bid auctions, the bidders cast their bids secretly before the bid deadline; then the auctioneer opens the bids and selects the winner according to the auction rules. The open-bid auctions are divided into English auctions and Dutch auctions, which are often used in commodity transactions among individuals. Compared with the open-bid auctions, the sealed-bid auctions only reveal the winning bid price, while the bid price of other bidders is kept secret. Sealed-bid auctions can effectively protect the anonymity of the bidders' identity and the privacy of the bid price. The efficiency of the sealed-bid auctions is also higher than that of the open-bid auctions. Therefore, sealed-bid auctions are mainly used for transactions between enterprises.

With the popularity of the Internet and the rapid development of e-commerce, e-auctions, as a new and

efficient form of auctions, provide a fair trading environment for buyers and sellers and are time- and cost-efficient. For the transactions of enterprise assets, sealed-bid e-auctions attract more bidders to participate, and the benefits of the owner of the goods (the seller) are better guaranteed. However, in the complex Internet environment, the defects of traditional e-auctions, such as privacy disclosure and centralized private verification, limit the application of e-auctions. Although most of the current researches on sealed-bid e-auctions are trying to use encryption technology and multiparty multiround computation to solve the untrustworthy problem of third-party auctioneers, it is still a great challenge to establish an all-in-one scheme to prevent information leakage and identify fraud and repudiation in the increasingly complex Internet environment.

In recent years, the blockchain technology was successfully applied in e-cash, intellectual property protection, evidence fixation, reputation systems, Internet of things (IoT), financial services, and energy trading [1–3]. Researchers have been trying to migrate e-auctions to blockchains. Theoretically speaking, the decentralization feature of blockchains can effectively remove the negative effects caused by the third-party auctioneer, and meanwhile, it can save the auction intermediary costs. The consensus mechanism, information encryption, smart contracts, and other technologies related to blockchains can automate the auction process without any deliberate intervention. Even if blockchain technology is faced with security issues such as majority attack and double spending, some studies have tried technologies such as machine learning to make blockchain-based applications more resilient against attacks [4, 5]. Therefore, the confidentiality of the auction data, the fairness of the auction activities, the auction commitment, and the nontampering of the auction results are well guaranteed.

In this paper, we proposed a sealed-bid e-auction scheme based on blockchains with commitment algorithm, smart contracts, and zero-knowledge proof to protect the bid information from leakage and verify the auction result with all bidders anonymously, which successfully implemented the secure and fair auction without the third-party auctioneer.

The paper was organized in the following sections.

In Section 2, the related studies were discussed and the gaps in related studies were analyzed. In Section 3, the main methods used in the sealed-bid e-auction scheme including the auction smart contract, bid price hiding algorithm, and bid result verification algorithm were introduced in detail. In Section 4, the process of the auction scheme was designed and all phases in the process were illustrated. In Section 5, we conducted an experiment to validate the proposed scheme. The experimental results were discussed in this section. In the last section of the paper, conclusive remarks and future study plan were provided.

For the sake of better readability, some important terms and variables used in the following sections are illustrated in advance in Table 1.

Table 1: Abbreviations and notations.

Abbr./ notation	Full name
P2P	Peer-to-peer communication
ECC	Elliptic curves cryptography
RSA	Rivest-Shamir-Adleman algorithm
DSA	Digital signature algorithm
ZK-STARK	A kind of zero-knowledge system: scalable transparent argument of knowledge
ZK-SNARK	A kind of zero-knowledge system: succinct noninteractive arguments of knowledge
b_i	The bidder with ID i
I	The set of all bidders' IDs
p^*	The winning price
p_i	The bid price of bidder i
r_i	The random blinding factor of bidder i
G, H	Two generating points on specific elliptic curves to encrypt bid price p_i
C_i	The commitment price of price p_i
C^*	The commitment price of the winning price
$\widehat{C}_i$	The differential commitment price of C^* and C_i
pk_s	The public key of the smart contract

2. Related Studies

At present, there have existed a lot of related studies on sealed-bid e-auctions.

Frankin and Reiter (1995) presented a distributed service for performing sealed-bid auctions. This service can issue secret bids to the service for an advertised auction. Once the bid period ends, the auction service opens the bids, which determines the winning bid. Using novel cryptographic techniques, the service is constructed to provide strong protection for both the auctioneer and trusted bidders [6]. Brandt et al. proposed an approach that does not rely on trusted third parties, for example, auctioneers. The proposed technique is based on EIGamal encryption to protect the bidders' privacy. However, all computation in the auction was only performed by the auctioneer and time-consuming [7, 8]. Bogetoft et al. combined knowledge from economics with Shamir secret sharing scheme to implement secure auctions without trusted auctioneers [9]. The linear secret sharing-based secure multiparty computation was used to implement the secure auction protocol instead of the trusted third party. However, the computation requires more interactions. Lee et al. proposed a securely sealed-bid auction scheme that uses the group signature scheme with the function of authenticated encryption. It was claimed to achieve the following goals: secrecy of bidding price, anonymity, verifiability, nonrepudiation, and better performance [10]. Cao tried bit commitment and blind signature technology to design an e-auction scheme based on untrusted third parties. Cao claimed that the e-auction scheme meets the demand of secure e-auction and it can withstand the conspiracy attack [11]. However, in this auction scheme, bidders may cast bid prices many times, which was not fully inconsistent with the auction rules. In addition, the auction result was announced by the winning bidder himself, which was absolutely unreliable. Sun et al. found that if the group manager has a valid group signature

of a member, without the member's secret key, he can forge a group signature on arbitrary message on behalf of the member. Therefore, Lee et al.'s group signature and auction scheme are insecure [12]. Wang et al. used identity-based group signature and provable secure sharing protocol to design the sealed e-auction scheme. The scheme aims at anonymity, robustness, unforgeability, verification, and privacy protection [13]. However, the scheme depended on the verification center, which acted as a kind of third-party auctioneer. It was argued that the fairness and reliability were not well guaranteed in this kind of centralized mode. Cheng et al. proposed a sealed-bid auction scheme based on an untrusted third party, which uses a digital signature to verify the bidders and encrypts the bid price to keep the secrecy and accuracy of auction [14]. This scheme implements anonymity, secrecy, and unforgeability. However, the winning bid price was verified and determined by the third-party auctioneer.

There have existed some blockchain-based sealed e-auction schemes. For example, Galal and Youssef proposed the sealed-bid auction on the Ethereum blockchain with smart contracts and zero-knowledge proofs. The proposed scheme implements the validity, fairness, secrecy of the auction transaction. However, the proposed scheme depended on the third-party auctioneer [15, 16]. Peng et al. designed a blockchain-based sealed-bid auction with concurrent signature. In their scheme, the fuzziness of concurrent signature is used to protect the privacy of bidders and hide the bid price [17]. However, the scheme was argued that the winning bid price was not reliably verified. Xiong proposed an anonymous e-auction protocol based on blockchains. In her protocol, the blind signature scheme was used to realize the anonymity of bid behavior [18]. However, this protocol was still based on the third-party auctioneer. Yu improved a two-party comparison protocol by zero-knowledge proof and proposed a sealed-bid blockchain auction scheme with semihonest judge parties. By using the blockchain as the infrastructure, the auction process and records cannot be tampered with and traceable to reduce the dependence on the third party and improve the fairness of the auction through bid security [19]. However, the semihonest judge party (the auctioneer) was still required to verify part of the zero-knowledge proof, and the partial security still depends on the honesty of the judge party.

According to the above literature review, the related studies still have some defects in sealed-bid auction schemes. (1) The risks from centralized transaction mode: as was discussed above, in traditional auctions, the whole transactions are in the control of auctioneers. It has been proved that the untrusted auctioneers may cause the bid price leakage and tamper with the auction results. In related studies, most e-auction schemes, even those based on blockchains, still took auctioneers as the transaction controllers. Therefore, the fairness and reliability of auctions were not perfectly guaranteed. (2) Incomplete price hiding: price hiding is the core of sealed-bid auctions. In most related studies, the bid price is protected by encryption. However, in the open phase, the bid price is decrypted and directly revealed for verification, which may cause price leakage and the benefits damage of the winning bidder.

3. Methods

3.1. Blockchains. Nakamoto proposed blockchains in his paper "Bitcoin: a peer-to-peer electronic cash system" [20]. As is stated, blockchain is a kind of distributed file system maintained by multiparty. With P2P communication, blockchains protect the data with encryption technology and consensus mechanism. Different from the traditional file systems, blockchains use chained file storages, put data records into blocks, and organize blocks into chained blocks by recording the hash value of the previous block in the header of each block (see Figure 1). Users (also called miners) can create multiple addresses on the blockchains, which are independent of the users' identity. The blocks are added by miners in the chain that solves complex puzzles whose transactional cost is lower than a specified target hash value. The copy of the added block is then broadcasted to every peer node in the chain. The block addition process is agreed upon and validated by the majority of the nodes in the chain. The agreement process is termed as consensus in the chain. If the majority of nodes agree to a common consensus, the block is added to the existing chain; otherwise, it is discarded [21]. Therefore, the creation process does not need the intervention of a third party. It is difficult to associate user identity through address information, which realizes better anonymity than traditional file systems. In practice, blockchains are divided into public blockchains, private blockchains, and consortium blockchains. Public blockchains and consortium blockchains have more blocks and stronger data tampering resistance, but they are puzzled by the lower operation efficiency. The private blockchains support highly efficient data operation, while the degree of decentralization is not as high as public blockchains and consortium blockchains. For e-auction, these three kinds of blockchains are all applicable.

In our proposed sealed-bid e-auction scheme, all auction data were encrypted and stored in the blockchain-based file systems.

3.2. The Smart Contract. Szabo invented smart contracts as a set of promises, specified in a digital form, including protocols within which the parties perform on these promises. From common law, economic theory, and contractual conditions often found in practice, four basic objectives of smart contracts are designed. The first of these is observability, the ability of the principals to observe the performance of the contract of each other or to prove their performance to other principals. A second objective, verifiability, is the ability of a principal to prove to an arbitrator that a contract has been performed or breached, or the ability of the arbitrator to find this out by other means. The third objective of contract design is privity, the principle that knowledge and control over the contents and performance of a contract should be distributed among parties only as much as necessary for the performance of that contract. The fourth objective is enforceability and at the same time minimizing the need for enforcement [22].

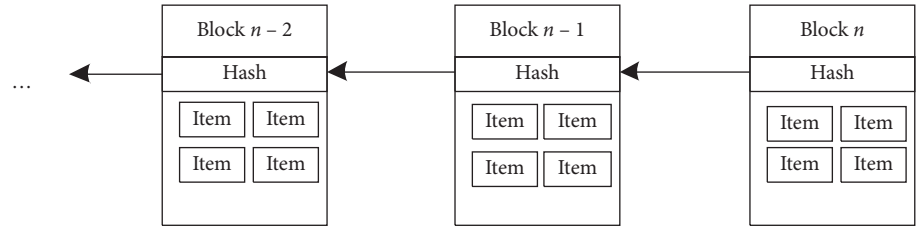

Figure 1: The file system of blockchains

Due to the lack of trusted execution environments, smart contracts have not been practiced widely until Ethereum integrated blockchains with smart contracts [23]. From then on, smart contracts become the core of new-generation blockchain-based applications which are not limited in the e-cash area. For example, Kumari et al. proposed a P2P secure energy trading scheme, ET-DeaL based on smart contract [24].

Smart contracts are usually implemented in programming languages such as Solidity [25] and Lua [26]. The developers define a set of rules as functions in smart contracts and then publish smart contracts on blockchains. That is, smart contracts are immutable and available for all users of blockchain applications. All users interact with smart contracts and call functions to fulfill the transactions. Since smart contracts are the consensus of all participants and are automatically running without any outer control, there is no opportunity for fraud behaviors to be executed.

The main actions in the proposed sealed-bid auction scheme are demonstrated in the following smart contract (see Algorithm 1).

3.3. Bid Price Hiding. We used cryptography commitment schemes to hide the bid price of bidders. Cryptography commitment schemes are a means of temporally hiding secret information so that it is verifiable in spite of the possible bias from either the prover (the party who commits to a value) or the verifier. The commitment scheme consists of three phases: setup, commitment, and verification. In the setup phase, the environment is set up, and keys are generated and published. During commitment, the prover commits to a message according to the proper algorithm and sends the commitment to the verifier. In the verification phase, the prover sends the information necessary for opening the commitment, and the verifier checks whether the commitment really is to the message that the prover claims it to be [27]. A well-designed cryptography commitment scheme should be characterized by the following features.

Hiding. Before the reveal of the commitment, the verifiers know nothing about data. There are three kinds of binding: (1) perfect binding means that even with infinite computing power, the prover cannot change his mind after committing to a message, (2) statistical binding means that if the prover has infinite computing power, he can cheat with negligible probability, and (3) computational binding means that unless the prover has very large computing resources, then the probability of being able to change the value of the message being committed to is negligible.

Binding. After the reveal of the commitment, the prover cannot explain data to other data. There are also three kinds of hiding: (1) perfect hiding means that a commitment to a message reveals no information about the message, even to an infinitely powerful verifier, (2) statistical hiding means that if the verifier has infinite computing power, he gets information about the message being committed to with negligible probability, and (3) computational hiding means that, for a polynomially bounded verifier, it is very difficult to guess what is inside the commitment.

It has been proved theoretically that the perfect commitment scheme with both perfect binding and perfect hiding is impossible. However, in the aspect of zero-knowledge proof for privacy protection, the first kind of commitment, which is supported by perfect hiding and computational binding, is usually used.

In cryptography commitment schemes, Hash commitment is the basic one, which uses a one-way hash function $H(v)$ to map the data v to a commitment. Based on the unidirectionality of $H(v)$, it is difficult to deduce the data v through $H(v)$, which implements a certain degree of data hiding. Based on the anticollision of one-way hash function, it is difficult to find different data v' to produce the same hash value, which implements a certain degree of data binding.

Hash commitment is simple in structure and easy to use, which meets the basic characteristics of cryptography commitment, ;and is suitable for applications with low requirements for data confidentiality. However, due to the lack of randomness, for the value v, the commitment $c = H(v)$ is fixed. Therefore, with powerful computation, the value v may be figured out through exhaustion computation. This kind of decryption is easy to implement in the current Internet environment. For applications that require higher data confidentiality, Hash commitment is not practical. In this paper, we proposed Pedersen's commitment [28] to hide the bid price.

The Pedersen commitment is based on elliptic curves cryptography (ECC) advised by Neal Koblitz and Victor S. Miller in 1985. ECC is a public key encryption technique in cryptography which depends on the elliptic curve theory which helps us to create faster, smaller, and most efficient or valuable cryptographic keys [29]. Compared with RSA and DSA algorithms, only 256-bit ECC is just equal to or comparable to the 3072-bit RSA key, the main reason behind keeping a short key is the use of great computational power and secure and fast connection. It is harder to break for

```
contract SealedBidAuction {
    struct Bid {
      bytes32 sealedBid;
      uint bidDeposit;
    }
    uint public biddingEndTime;
    uint public revealEndTime;
    function bid(bytes32 _sealedBid)
      public
      payable
      onlyBefore(biddingEndTime)
    {...}
    function open(uint[] _values, bytes32[] _secret)
      public
      onlyAfter(biddingEndTime)
      onlyBefore(revealEndTime)
    {...}
    function finish()
      public
      onlyAfter(revealEndTime)
    {...}
}
```

Algorithm 1: The sealed-bid auction smart contract.

hackers compared to RSA and DSA, which means that the ECC algorithm ensures or secures the website and infrastructure safety than traditional methods in a more secure manner in the future.

The Pedersen commitment cryptography function is defined in equation (1). By introducing the random blinding factor r, even if the private data v remains unchanged, the final commitment c will change according to the change of r, which implements the hiding of data. G and H generated by smart contracts are two generating points on specific elliptic curves, which are consensus information to all auction parties.

$$C(p, r) = r \times G + p \times H. \tag{1}$$

In our sealed-bid e-auction scheme, the Pedersen commitment scheme worked in the following steps:

(1) The bidder b_i got a random blinding factor r_i and called the above Pedersen commitment function $C(p_i, r_i)$ to produce the commitment price C_i. $i \in I$, where I was the set of the IDs of all bidders.

(2) The bidder b_i published C_i to the blockchain and sent $E(p_i, r_i, pk_s)$ to the smart contract account. E was the encryption function to encrypt p_i and r_i with pk_s, where pk_s was the public key of the smart contract.

(3) When the bid deadline arrived, the smart contract opened the commitment. The commitment C^* bound to the winning price p^* was revealed and the differential commitment $\widehat{C}_i$ was sent to all bidders. $\widehat{C}_i$ was defined in equation (2), which was sent to bidder b_i.

$$\begin{aligned}\widehat{C}_i &= C^* - Ci = (r^* - r_i) \times G + (p^* - pi) \times H \\ &= r_i^* \times G + p_i^* \times H.\end{aligned} \tag{2}$$

If $p_i^* \geq 0$, then $p^* > p_i$.

3.4. Verification of Bid Result. In practice, the additive homomorphism of Pedersen's commitment is integrated with Bulletproofs, an outstanding zero-knowledge proof protocol, to prove the binding relations of different values. Bulletproofs were proposed by Benedikt et al. (2018) as a new noninteractive zero-knowledge proof protocol with very short proofs and without a trusted setup [30]. It is proved that Bulletproofs have better performance than ZK-SNARKs [31] and ZK-STARKs [32] and are very useful for encrypted currency. Bulletproofs can prove that the transaction amount is in a given positive range, which is essential to verify the transaction. Therefore, we can use the Pedersen commitment algorithm to hide the real bid price and verify the higher biding price with the differential commitment price $\widehat{C}_i$ in equation (2) by Bulletproofs, because it is very easy to prove $p_i^* \in [0, 2^n)$ (i.e., $p_i^* \geq 0$) with Bulletproofs and $\widehat{C}_i$. Therefore, each bidder can verify that p^* is higher than his bid price p_i.

The verification operation is shown as follows:

(1) Bidder b_i recomputed the differential commitment price $\widehat{C}_i'$ with the published C^* and his own commitment price C_i, where $\widehat{C}_i' = C^* - C_i$.

(2) Bidder b_i compared $\widehat{C}_i'$ with $\widehat{C}_i$ that was produced and distributed by the smart contract.

(3) If $\widehat{C}_i' = \widehat{C}_i$, C^* was accepted. Then bidder b_i used Bulletproofs and $\widehat{C}_i$ to prove p^* to be higher than his own bid price p_i and returned the proof result to the smart contract.

(4) When all bidders returned the proof results, the smart contract announced that the auction was successfully completed.

In the above steps, since all bidders published the commitment price on the blockchain, if one bidder changed (p, r) to make a new commitment price against the winning commitment C^*, the smart contract and other bidders would be aware of his fraud behavior. The dishonest bidder would be regarded as an untrusted party and punished according to the auction rules. For example, the untrusted bidder's bid security would be confiscated and his permission to auction would be frozen for a period of time. For the owner of goods, since the smart contract was the consensus of all users of the auction system and automatically executed without outer control, the auction result was also accepted by the owner of goods. So far, the decentralized and completely privacy-protected sealed-bid e-auction was successfully implemented.

4. The Auction Process

The process of the decentralized sealed-bid e-auction was divided into six phases: register, publish, bid, open, verify, and finish. In the auction scheme, there were four kinds of parties: owner of goods, bidders, the smart contract, and the blockchain. The owner of goods published the goods information to the blockchain, and then the bidders cast their bid price before the bid deadline. The smart contract provided functions to support the actions in the above phases.

The flowchart of the auction process is shown in the sequence diagram in Figure 2.

4.1. The Register Phase. The users including the owner of goods and all bidders should register in the sealed auction system. The register function in the smart contract returned the user IDs and public and private keys to registered users. When users got these registration data, they encrypted the IDs with the public key of the smart contract and saved the encrypted IDs in the blockchain.

4.2. The Publish Phase. After registration, the owner of goods called the publish() function in the smart contract to publish the goods information. In publish() function, the following activities were conducted:

(1) The smart contract verified the user ID and returned the publish permission to the owner of goods.

(2) The owner of goods sent the goods introduction, auction starting time t_1, auction ending time t_2, bid security requirement m, the smallest number of bidders n, and encrypted reserve price p_r (encrypted by the public key of the smart contract) to the smart contract and saved them in the blockchain. That is, all information was the consensus except the reserve price.

4.3. The Bid Phase. From time t_1, the registered bidders who were interested in the goods were permitted to bid. The bid() function in the smart contract was responsible for the following bidding tasks.

(1) The bidders' identity was also verified by the smart contract like the goods' owner.

(2) The bidders saved the caution deposit m to the account appointed and supervised by the smart contract.

(3) Each bidder b_i provided the bid price p_i and a random number r_i that were encrypted by the public key of the smart contract and saved them in the blockchain. The bid price p_i will never be revealed by the smart contract.

(4) Each bidder b_i called the Pedersen commitment function to get the commitment price C_i and saved it in the blockchain. Commitment price C_i was encrypted by the private key of b_i. That is, all bidders and the owner of goods can get the information of C_i by decrypting it with the public key of b_i.

4.4. The Open Phase. When time t_2 arrived, the smart contract conducted the following activities:

(1) The smart contract counted the bidders attending the auction and checked all bid prices in the auction. If the number of bidders was smaller than n, or all bid price was smaller than the reserve price p_r, the auction was announced failed. Otherwise, the subsequent activities were taken.

(2) All bid price was sorted and the highest bid price p^* was selected as the winning bid price.

(3) The commitment price C^* bound to p^* was published to the blockchain by the smart contract.

(4) Each differential commitment price $\widehat{C}_i$ was calculated and encrypted with the public key of each bidder by smart contract and sent back to each bidder.

4.5. The Verify Phase. When each bidder b_i got C^* and $\widehat{C}_i$, he recalculated the differential commitment price $\widehat{C}'_i = C^* - C_i$ and compared $\widehat{C}_i$ with $\widehat{C}'_i$. If $\widehat{C}'_i = \widehat{C}_i$, $\widehat{C}_i$ was successfully verified by bidder b_i. Then all bidders used Bulletproofs protocol to prove p^* with $\widehat{C}_i$ without leaking any information about the winning bid price p^*.

4.6. The Finish Phase. After all bidders were verified and accepted p^*, the smart contract asked the winning bidder to pay the rest of the payment for goods $(p^* - m)$ to the appointed account and then transferred the full payment p^* to the owner of goods. The bid security of the other bidders was also returned to the bidders' own accounts.

5. Experiments and Discussion

In order to verify the feasibility of the proposed scheme, we built an Ethereum-like simulation experiment to test the main algorithms of the proposed sealed-bid auction scheme. The simulation environment was composed of 30 computers

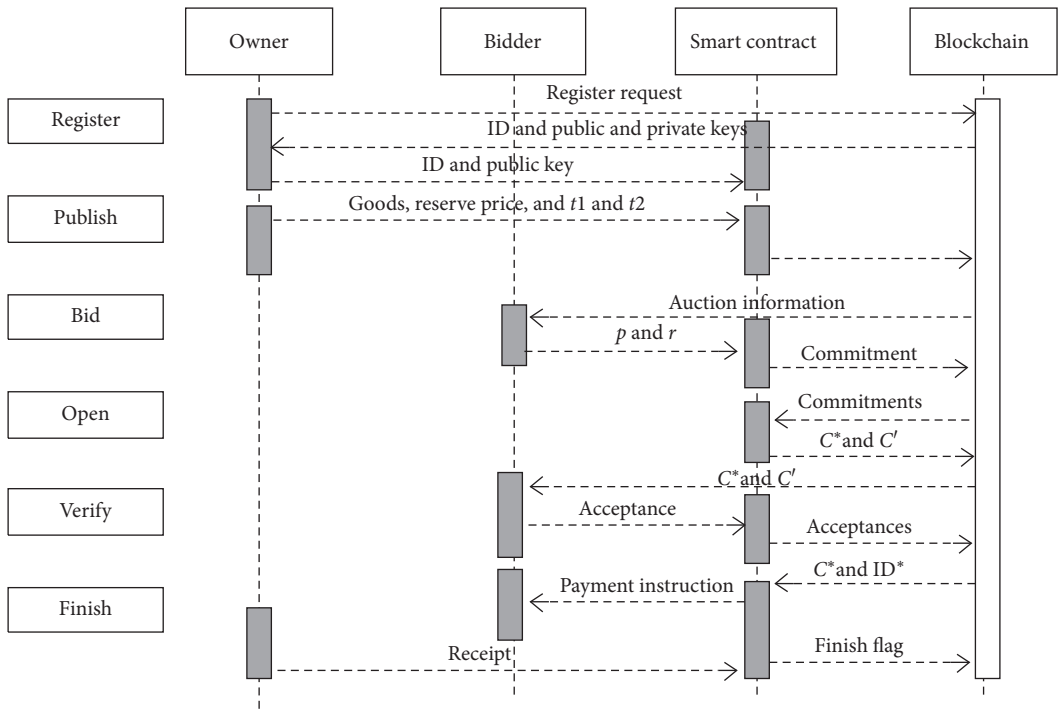

Figure 2: The process of the decentralized sealed-bid e-auction.

(blocks). The configuration of each node computer is shown in Table 2.

The application was coded in Java development kits (JDK1.8) and Java pairing-based cryptography library (JPBC 2.0.0). The smart contract was coded in Solidity and Web3J and tested in Truffle.

We conducted 6 auction transactions with a different number of bidders. In each auction transaction, the goods' owner published the encrypted goods' information privately and secretly. Each bidder submitted his bid price separately.

5.1. Performance Analysis of the Scheme. In each auction transaction in the experiment, the execution time of each transaction phase was recorded (see Table 3).

We calculated the correlation coefficients between the number of bidders and the execution time in different phase (see Table 4).

With the correlation coefficients, we found that the execution time of open and finish operations grew significantly with the increase of the number of bidders. It hinted that if more bidders attended the auction, the open and finish operation would spend more time. However, for publish, bid, and verify operations, the execution time remained relatively stable with different number of bidders. We conducted Chi-square test on the contingency table of execution time in publish, bid, and verify phases with a different number of bidders. The p value was 0.99, which hinted that there were no significant differences between the execution time in these phases. It meant that since these 3 operations were independently executed by each bidder, the execution time of these operations was not influenced by the number of bidders.

Table 2: Configuration of computers (blocks).

Parameter	Value
CPU	1.2 GHz
Memory	4 G
Bandwidth	1000 M
OS	CentOS 7.3
Hard disk	256 G

Table 3: Execution time of each phase with different number of bidders (in milliseconds).

Number of bidders	Publish	Bid	Open	Verify	Finish
3	45.6	35.7	72.4	60.3	60.9
5	42.6	32.7	104.5	65.4	77.3
7	42.9	35.4	135.7	57.4	107.8
15	43.2	28.2	265.5	63.6	195.2
25	46.2	32.1	404.7	59.4	297.5
29	46.5	33.9	482.4	60.1	319.9

Table 4: Correlation coefficients between the number of bidders and the execution time in different phase.

	Publish	Bid	Open	Verify	Finish
Number of bidders	−0.39	−0.3	0.99	−0.21	0.99

We also estimated the mean gas value of each phase operation (see Table 5). The largest gas value was about 6 million, which was far smaller than the current gas limit (12 million) of Ethereum. It hinted that the proposed scheme could be deployed on Ethereum.

Table 5: The gas value of each phase operation in the proposed auction scheme.

Publish	Bid	Open	Verify	Finish
2,746,246	2,246,142	6,362,528	3,432,558	4,386,935

Table 6: Comparison with related blockchain-based schemes

Scheme	Galal and Youssef [15]	Peng et al. [17]	Xiong [18]	Yu [19]	The proposed*
Decentralization (without auctioneer)	No	Yes	No	Partial	Yes
Anonymity	Yes	Yes	Yes	Yes	Yes
Authentication	Yes	Yes	Yes	Yes	Yes
Unforgeability	Yes	Yes	Yes	Partial	Yes
Nonrepudiation	Yes	Yes	Yes	Partial	Yes
Winning price validation	Yes	No	Yes	Yes	Yes

5.2. Comparison Analysis with Related Blockchain-Based Works. In each transaction of auctions in the experiment, all bid prices and bidders' identities were revealed to the observers for the validation of the proposed scheme. Through the experiment records, we confirmed the following:

(1) The encrypted goods information was successfully published to all block nodes.

(2) Each bid price was successfully encrypted as the commitment price and published to all block nodes.

(3) All bidders verified the winning price without any knowledge of the bid price of other bidders.

(4) The winning price and the winning bidder were right confirmed by all transaction participants.

We compared four recent representative related works in six metrics including decentralization, anonymity, authentication, unforgeability, nonrepudiation, and winning price validation. The result is shown in Table 6.

Galal and Youssef [15], Xiong [18], and Yu [19] provided well-designed schemes based on blockchain technologies. These 3 schemes show good performance in most metrics. However, they are based on their party auctioneers, which means that the schemes are subject to information leakage risks. Peng et al. [17] proposed an innovative scheme without auctioneer, which makes a breakthrough in the sealed-bid auction mechanism design. But in his scheme, the winning price is revealed to all bidders for the auction result validation. Even all participants of the auction confirm the result without any knowledge of the winning bidder's identity, it is not reasonable to reveal the winning price to the public.

In summary, through the experiment, the proposed scheme successfully performed the fair, secure, and reliable sealed-bid auction without the third-party auctioneer. It implemented a kind of decentralized auction with the help of blockchain technologies.

6. Conclusion and Future Work

Compared with the related sealed-bid auction schemes, the proposed scheme in this paper used the features of blockchain technologies to realize decentralized auctions. The risks from the third-party auctioneers were well eliminated. In summary, the proposed sealed-bid e-auction scheme showed the following features:

(1) *Sealability*. All information in the auction transaction was encrypted by the public keys of the smart contract, owner, and bidders, which prevented the information from leakage. The bid price was only passed to the smart contract other than published on the blockchain. In addition, the bid price was mapped to a commitment price by the Pedersen commitment function. For all users getting the commitment price, they can never get the real bid price of bidders.

(2) *Fairness*. All bidders were equally treated by the smart contract. They got all commitment prices and the winning commitment price C^*. Then, they verified the auction result autonomously. If bidders tried to tamper with the auction result, their auction security would be confiscated and their permissions to the auction transaction were also frozen or canceled. The punishment was conducted automatically by the smart contract.

(3) *Validity*. The smart contract selected the winning bid price and the related bidder as the auction result, which obeyed the basic rule of the first-price sealed auction.

(4) *Nonrepudiation*. All information in the auction transaction was saved in the blockchain and can never be denied under the consensus mechanism of blockchains.

(5) *Decentralized Verification*. All bidders can verify and prove the auction result with zero-knowledge proof protocol (Bulletproofs). None of them can deny the bid price.

(6) *Cost-Effective*. The scheme was free of the cost of the third-party auctioneer, which made the biggest benefits of all auction parties.

It should be noted that the proposed scheme has limitations in running performance. As was discussed in Section 5.1, the execution time of the open phase and finish phase was determined by the number of bidders. It means that the auction would become a time-consuming work if conducted in the open platforms such as Internet. In future studies, we will focus on the improvement of algorithms of the two auction phases and test the scheme in real blockchain environments. In addition, we will also investigate blockchain technologies other than Ethereum, which can help us protect the privacy of bids from all parties with lower computation resource requirements.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

The authors have read and agreed to the published version of the manuscript.

Acknowledgments

The authors would like to acknowledge Liaoning Normal University for the lab facilities and the necessary technical support. This research was funded by the National Natural Science Foundation of China, under Grant no. 62072221.

References

[1] S. Tanwar, S. Kaneriya, N. Kumar, and S. Zeadally, "ElectroBlocks: a blockchain-based energy trading scheme for smart grid systems," *International Journal of Communication Systems*, vol. 33, no. 15, p. e4547, 2020.

[2] A. Kumari, R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "When blockchain meets smart grid: secure energy trading in demand response management," *IEEE Network*, vol. 34, no. 5, pp. 299–305, 2020.

[3] A. Kaur, A. Nayyar, and P. Singh, "Blockchain: a path to the future," *Cryptocurrencies and Blockchain Technology Applications*, John Wiley & Sons, Hoboken, NJ, USA, pp. 25–42, 2020.

[4] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W.-C. Hong, "Machine learning adoption in blockchain-based smart applications: the challenges, and a way forward," *IEEE Access*, vol. 8, pp. 474–488, 2020.

[5] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020.

[6] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction service," *IEEE Transactions on Software Engineering*, vol. 22, no. 5, pp. 302–312, 1996.

[7] F. Brandt and T. Sandholm, "Efficient privacy-preserving protocols for multi-unit auctions," in *Proceedings of the 2005 Financial Cryptography & Data Security, Financial Cryptography and Data Security*, pp. 298–312, Springer, Roseau, Dominica, February-March 2005.

[8] F. Brandt, "How to obtain full privacy in auctions," *International Journal of Information Security*, vol. 5, no. 4, pp. 201–216, 2006.

[9] P. Bogetoft, I. Damgård, T. Jakobsen, K. Nielsen, J. Pagter, and T. Toft, "A practical implementation of secure auctions based on multiparty integer computation," *Financial Cryptography and Data Security* in *Proceedings of International Conference on Financial Cryptography & Data Security*, vol. 4107, pp. 142–147, Springer, Anguilla, British West Indies, February-March 2006.

[10] C.-C. Lee, P.-F. Ho, and M.-S. Hwang, "A secure e-auction scheme based on group signatures," *Information Systems Frontiers*, vol. 11, no. 3, pp. 335–343, 2009.

[11] G. Cao, "Electronic auction scheme based on trustless third-party," *Computer Engineering*, vol. 36, no. 20, pp. 140–144, 2010.

[12] Y. Sun, Y. Sun, M. Luo, L. Gu, S. Zheng, and Y. Yang, "Comment on Lee et al.'s group signature and e-auction scheme," *Information Systems Frontiers*, vol. 15, no. 1, pp. 133–139, 2013.

[13] X. Wang, X. L. Zhang, M. Gao, and X. Chen, "An efficient sealed electronic auction scheme," *Journal of Qingdao University (Natural Science Edition)*, vol. 28, no. 1, pp. 64–69, 2015.

[14] W. Y. Cheng, Y. Y. Dong, and J. G. Han, "A simple and efficient sealed-bid electronic auction scheme," *Computer Engineering*, vol. 40, no. 3, pp. 171–174, 2014.

[15] H. S. Galal and A. M. Youssef, "Verifiable sealed-bid auction on the Ethereum blockchain," in *Proceedings of the 2018 Financial Cryptography*, pp. 265–278, Springer, Nieuwpoort, Curaçao, March 2018.

[16] H. S. Galal and A. M. Youssef, "Succinctly verifiable sealed-bid auction smart contract," in *Proceedings of the 2018 Data Privacy Management, Cryptocurrencies And Blockchain Technology, Lecture Notes in Computer Science*, pp. 3–19, Springer, Barcelona, Spain, September 2018.

[17] Y. Peng, Y. Gao, and J. X. Wu, "A privacy preserving sealed-bid auction scheme based on block chains," *Cyberspace Security*, vol. 9, no. 8, pp. 1–7, 2018.

[18] J. Xiong, *Research on Anonymous Electronic Auction Protocol Based on Blockchain*, Jinan University, Guangzhou, China, 2019.

[19] R. Yu, *Research on the Sealed-Bid Auction Scheme for Blockchain Based on Secure Comparison Protocols*, Northwest A&F University, Xianyang, China, 2019.

[20] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Cryptography Mailing List*, 2009, https://bitcoin.org/bitcoin.pdf.

[21] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," *IEEE Access*, vol. 8, pp. 54371–54401, 2020.

[22] N. Szabo, "Smart contract: building blocks for digital markets," 1996, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[23] V. Buterin, "A next-generation smart contract and decentralized application platform," 2013, https://ethereum.org/en/whitepaper.

[24] A. Kumari, A. Shukla, R. Gupta, S. Tanwar, S. Tyagi, and N. Kumark, "ET-DeaL: a P2P smart contract-based secure energy trading scheme for smart grid systems," in *Proceedings of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1051–1056, Toronto, Canada, July 2020.

[25] "Solidity," 2020, https://github.com/ethereum/solidity/releases/tag/v0.8.0.

[26] "Lua," 2020, https://www.lua.org/versions.html#5.4.

[27] L. Kamm, "MTAT.07.006 research seminar in cryptography commitment schemes," 2006, https://courses.cs.ut.ee/2006/crypto-seminar-fall/files/kamm1.pdf.

[28] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proceedings of the 11th Annual International Cryptology Conference, Advances in Cryptology-CRYPTO'91*, pp. 129–140, Santa Barbara, CA, USA, August 1991.

[29] V. S. Miller, "Use of elliptic curves in cryptography," in *Proceedings of Advances in Cryptology-CRYPTO'85*, pp. 417–426, Santa Barbara, CA, USA, August 1985.

[30] B. Benedikt, B. Jonathan, B. Dan, P. Andrew, W. Pieter, and G. M. Bulletproofs, "Short proofs for confidential transactions and more," in *Proceedings of the IEEE 2018 IEEE Symposium on Security and Privacy (SP)*, pp. 315–334, San Francisco, CA, USA, May 2018.

[31] J. Groth and M. Maller, "Snarky signatures: minimal signatures of knowledge from simulation-extractable SNARKS," in *Proceedings of the 2017 International Cryptology Conference, Advances in Cryptology-CRYPTO 2017*, pp. 581–612, Springer, Santa Barbara, CA, USA, August 2017.

[32] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," Cryptology ePrint Archive: Report 2018/046, 2018, https://eprint.iacr.org/2018/046.pdf.