applied sciences

MDPI

Article

Research on Blockchain-Based E-Bidding System

Dan Wang, Jindong Zhao * and Chunxiao Mu

School of Computer and Control Engineering, Yantai University, Yantai 264005, China; wangdan9651@gmail.com (D.W.); mcx@ytu.edu.cn (C.M.)
* Correspondence: zhjdong@ytu.edu.cn

Abstract: In the field of modern bidding, electronic bidding leads a new trend of development, convenience and efficiency and other significant advantages effectively promote the reform and innovation of China's bidding field. Nowadays, most systems require a strong and trusted third party to guarantee the integrity and security of the system. However, with the development of blockchain technology and the rise of privacy protection, researchers has begun to emphasize the core concept of decentralization. This paper introduces a decentralized electronic bidding system based on blockchain and smart contract. The system uses blockchain to replace the traditional database and uses chaincode to process business logic. In data interaction, encryption techniques such as zero-knowledge proof based on graph isomorphism are used to improve privacy protection, which improves the anonymity of participants, the privacy of data transmission, and the traceability and verifiable of data. Compared with other electronic bidding systems, this system is more secure and efficient, and has the nature of anonymous operation, which fully protects the privacy information in the bidding process.

Keywords: blockchain; privacy protection; E-bidding system; smart contract; zero-knowledge proof; hyperledger fabric

Citation: Wang, D.; Zhao, J.; Mu, C. Research on Blockchain-Based E-Bidding System. *Appl. Sci.* **2021**, *11*, 4011. https://doi.org/10.3390/app11094011

Academic Editor: Luis Javier Garcia Villalba

Received: 31 March 2021
Accepted: 25 April 2021
Published: 28 April 2021

1. Introduction

Blockchain is a decentralized public ledger based on P2P networks, which has attracted wide attention in distributed application systems in recent years. In this technology, a tamper-resistant digital platform for data storage and sharing is realized by applying the chain-block structure and establishing a trusted consensus mechanism to synchronize data changes. At the same time, the decentralization, traceability and immutability of on-chain information storage makes blockchain a trusted machine with high reliability and security. Based on these characteristics, researchers began to analyze the application of blockchain in various fields, such as the Internet of Things, supply chain management, voting system [1,2] and bidding system. Blockchain in application can improve the availability of data and reduce costs, while maintaining the openness and transparency of the application [3,4].

In recent years, electronic bidding (E-bidding) has become an efficient and convenient service, which aims to provide an open and safe bidding environment for suppliers to protect the public interest. Tendering and bidding is a kind of commodity trading behavior; in simple words, it is an organized selection of excellent transaction ways by the tenderee. Compared with traditional offline bidding, it has an obvious difference in efficiency, information collection and other aspects, and is better in the identity authentication of the bidding object, confidentiality of the bidding content, fairness of the bidding process and other aspects.

Emerging blockchain technology combined with smart contracts could revolutionize traditional E-bidding systems in a decentralized and autonomous manner. It paves the way for a secure, immutable and auditable E-bidding process, while maintaining strong accuracy and completeness.

At present, there are also blockchain-based E-bidding designs, but they are limited to using the characteristics of the blockchain to achieve the preservation of information

in all aspects of the whole bidding process. In the process of preserving information, the blockchain may need to receive sensitive data to execute a smart contract. Therefore, it is crucial to ensure the privacy and authenticity of the data sent to the blockchain, so that everyone can verify the data without compromising sensitive information.

This paper presents a system framework that uses blockchain technology and smart contract to solve the privacy and security problems of E-bidding systems. Firstly, the overall architecture of E-bidding systems based on blockchain technology is described. Afterwards, the implementation process of tendering, bidding and bid evaluation is studied. Finally, the paper analyzes the possible problems of the E-bidding system, and provides a new solution for the reform of the E-bidding system based on blockchain technology.

1.1. Related Work

1.1.1. E-Bidding

In 2008, C. Fan et al. proposed a new E-bidding protocol [5], in which each bidder could join different bidding projects only after one round of registration, effectively reducing the cost of multiple registration in traditional bidding activities and enhancing the anonymity of bidders. In 2013, Xu Jing et al. proposed a novel tendering and bidding system based on cloud computing [6], which created a new layer based on cloud computing by establishing a reliable database. V.A. Trinh et al. [7] proposed in 2019 that in E-bidding applications, only one responsible person is able to check the validity of the signer's signature to avoid information leakage and other undesirable phenomena. In 2020, Tang Jun proposed a bidding system based on Ethereum smart contract technology [8] and discussed the ultimate goal of unmanned intelligent review by introducing deep learning methods.

1.1.2. Blockchain-Based E-Bidding

With the development of blockchain technology, many E-bidding schemes based on blockchain have been proposed. For example, in 2018, F.S. Hardwick et al. proposed to apply the concept of smart contract to government bidding [9], making it possible to have a fair, transparent and independently auditable government bidding plan. In 2018, H.S. Galal et al. proposed a smart contract protocol for a succinctly verifiable sealed-bid auction on the Ethereum blockchain [10]. In addition, it shows how zk-SNARK can be utilized to build Vickrey auction on top of Ethereum blockchain. P. Manimaran et al. introduced a blockchain-based E-bidding system [11] in 2019. In this model, there is no need for a third party. Smart contract will handle all bidding transactions, and the system makes sure that the integrity of the bidding process is preserved. In 2020, E.O. Blass et al. proposed a system to securely implement a variety of sealed-bid auctions through building blocks [12], which can improve efficiency, achieving low interactivity between parties to support blockchains or other scenarios where multiple rounds are time-consuming. In 2020, X.C. Li proposed a blockchain-based credible e-bidding system (BCES) [13] to address operational compliance, multi-party coordination and cybersecurity problem in the process of distribution, verification and backtracking of bidding data files. In 2021, A. Sarfaraz et al. proposed a blockchain-based framework for an open-bid auction system, in which privacy and security constraints are considered with different cryptographic primitives [14]. It integrates the blockchain structure by replacing the original chain structure with a tree structure. The security between auctioneer and bidder is enhanced by elliptic curve cryptography (ECC) and a dynamic cryptographic accumulator encryption algorithm. In 2021, I. Omar et al. proposed a solution based on the Ethereum blockchain in [15] that uses Ethereum smart contracts, decentralized storage systems and trusted Oracle to capture interactions between auctioneers and bidders in order to ensure data integrity and transparency and to eliminate intermediaries.

1.2. Contribution

At present, the E-bidding system is becoming more and more perfect, but there are still some problems, such as information opacity, resource sharing difficulty, high credit cost and data privacy insecurity. Aiming at these problems of traditional E-bidding platforms, this paper uses the characteristics of openness, transparency, tamper-proofing, high trust and traceability of blockchain technology to construct a new E-bidding system. The system uses Hyperledger Fabric to replace a trusted third party, and uses a chaincode to implement business logic, which can achieve the goal of reducing costs and improving data verifiability.

Secondly, this paper combines blockchain technology and privacy protection mechanism to encrypt and store bidding information on the chain through smart contract, so that the integrity of bidding can be generally guaranteed. In the system, the zero-knowledge proof protocol is used to verify the identity of participants and ensure the anonymity of users, as well as the confidentiality and review of data [16].

In summary, the work has made the following contributions:

- An E-bidding framework based on blockchain and smart contract is proposed to be suitable for large-scale bidding.
- A privacy protection approach for E-bidding systems is proposed. The non-linkable zero-knowledge proof protocol helps preserve the anonymity of the sender while protecting the anonymous receiver of the transaction.

2. Preliminaries

In this section, the traditional E-bidding system has been adjusted to make the following preliminaries.

2.1. Consortium Blockchain

Most of the traditional blockchain applications, such as Bitcoin, Ethereum, etc., are based on completely open and transparent permissionless blockchain. The public blockchain is a highly decentralized distributed ledger, which is convenient for any node to read data, send transactions, and freely enter and exit the blockchain network, and the transactions can be effectively confirmed. However, it has high latency, low efficiency, and lacks corresponding supervision mechanisms, which brings potential privacy threats. Therefore, it is not suitable for such activities as bidding.

The private blockchain is a non-public "chain" in which write permissions of each node are subject to internal control, while read permissions are selectively opened to the outside as required. Applicable to the internal data management and audit of specific organizations, only internal authorized users can access the blockchain data. Public tenders require the participation of multiple institutions, so private chains are not qualified for this scenario.

Consortium blockchain, also known as "permissioned chain", is a semi-closed blockchain, which refers to a blockchain that is jointly managed by multiple industry institutions. Only members of the consortium can read, write and send all or part of the data [17]. It fundamentally closes the channels for unauthorized nodes to access data, realizes complete authority control and security guarantee, and significantly reduces the risk of blockchain privacy leakage [18]. Moreover, the transaction operation performance of the consortium blockchain is high, the transaction is cost-free, and the smart contract can be upgraded and extended easily. Since the E-bidding system needs to strictly control the anonymity of participants and the encryption of transaction information according to the requirements [19], the consortium blockchain technology is more suitable for the system.

2.2. Hyperledger Fabric

Hyperledger is the most representative consortium blockchain at present. Hyperledger Fabric (HLF), the cornerstone of the Hyperledger project, is an open-source enterprise-level

licensed Distributed Ledger Technology (DLT) [20] platform, which was originally created by IBM and Digital Asset.

In the HLF platform, all participants must be authenticated before they can participate in the transaction on the blockchain. On the one hand, HLF supports smart contracts such as Ethereum, which describe and execute the application logic of the system. On the other hand, Hyperledger is different from public blockchains such as Ethereum or Bitcoin.

The following points describe how to mitigate the limitations of an Ethereum-based system in an HLF-based framework:

1. In the HLF framework, traditional programming languages such as Java and Go can be used to write smart contracts for chaincode.
2. All the chaincodes in the framework run on the Dockers container. The modular nature of the different components and chaincodes in the container enables it to achieve flexibility, versatility and reusability of various goals.
3. HLF also introduces the concept of multichannel, which enables different services to run on different channels and ensures data isolation between nodes connected to the channel. As a result, HLF does not require anonymous miners to verify the transaction, nor does it require expensive mining calculations to submit the transaction; that is, it does not require related currencies as incentives. Therefore, it not only saves time and money, but also increases the scalability of the transaction.
4. As the open-source framework of the consortium blockchain, Hyperledger is biased towards the characteristics of the consortium architecture in design. All or part of the permissions are only available to members of the consortium. Usually, according to the consortium consensus designated several nodes to record the ledger, other nodes only participate in the transaction and read the relevant information authority. Therefore, the consortium blockchain can achieve higher transaction efficiency and meet the needs of decentralization at the same time. In addition, the privacy of data can be protected to a certain extent.

To sum up, Fabric is one of the platforms with better performance in transaction processing and confirmation delay. It realizes smart contract and transaction privacy and confidentiality.

HLF has a flexible and modular architecture. It supports open and standard protocols [21] and has different functions. The HLF has the following significant features:

- Chaincode: Similar to smart contracts in the Ethereum network, it is a script written in a more advanced language, and all transactions executed are permanently stored in a ledger, where all participants can view this information. Chaincode is a superset of smart contracts; that is, smart contracts manage the business logic, and chaincode manages the smart contracts defined within them.
- Channel: A dedicated communications subnet used to transfer confidential data between multiple network members. Activities on a channel are visible only to associated and authorized entities.
- Endorser: The endorser invokes chaincode to validate the transaction and return the result of the endorsed transaction to the application.
- Membership services provider (MSP): MSP is used to identify a trusted certificate authority (CA) to define members of the trust domain, to provide authentication and access control by issuing and verifying certificates, and to determine the specific roles (members, administrators, etc.) that members may play in the blockchain network.

These characteristics of Fabric make it a highly scalable system. It is a highly modular and configurable architecture that can provide diversity, innovation and optimization for businesses of many fields, so it can support various industrial applications from finance, supply chain, healthcare to tendering and bidding.

The HLF maintains a business network that connects the different businesses of stakeholders through the Fabric software development kit (SDK) in the bidding process. Then, each bidder needs to be connected to the framework through client nodes. Bidding

organizations collect and submit documents through the client to the SDK within the framework. Submitted documents are automatically checked by chaincode. The client from the tenderee and the bidder and peer node members must be registered with the MSP and require a digital certificate from the CA. At the commencement of the transaction, the bidder will collect tender documents, review requirements and prepare bidder documents. Figure 1 shows the process framework and its different components of the E-bidding system with a typical HLF:

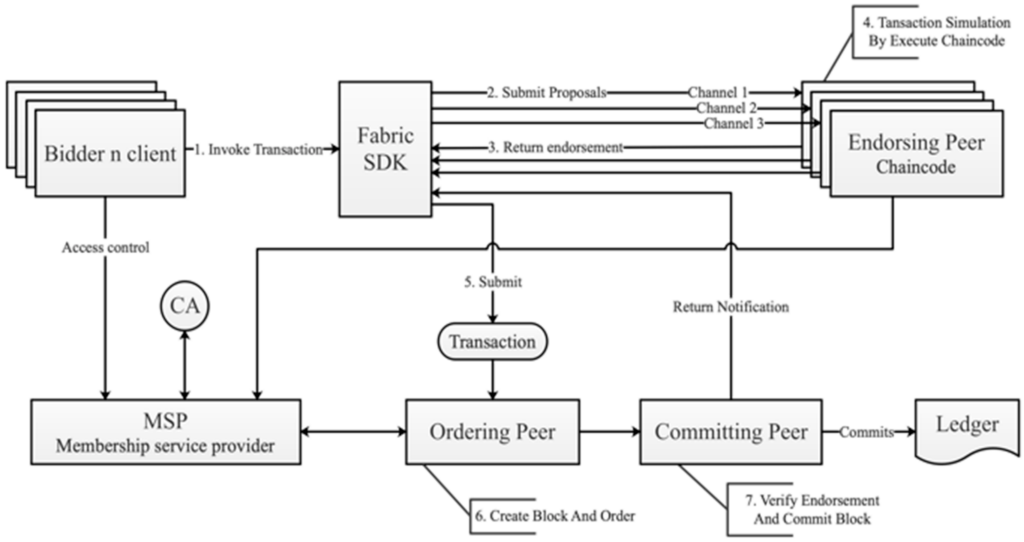


Figure 1. The framework and process of E-bidding system with HLF.

The discussion will follow the following brief steps:

Step 1. The bidder initiates the transaction by sending a request to the HLF-based application client.

Step 2. The client invokes SDK to submit the transaction proposals to the endorsing peer.

Step 3. These endorsement peers receive the transaction proposals, simulate the transaction by executing chaincode specified by the transaction, and verify it with business logic.

Step 4. After verification, the endorsing peer executes the transaction in the ledger and returns the response result to the Fabric platform. The bidder receives and verifies the response of the endorsing peer.

Step 5. At the same time, Fabric platform combines transaction with endorsement, and broadcasts it to the ordering peer.

Step 6. The ordering peer checks the endorsements and orders the transactions sequentially, packs a transaction block for each channel through the consensus mechanism and delivers it to the committing peer [22].

Step 7. The committing peer verifies the transaction in the block by checking the signature and version information, and then submits the transaction to the ledger and notifies the Fabric platform.

In the transaction process, Steps 1, 2, 3, and 4 represent the endorsement process, Steps 5 and 6 are similar to the ordering process, Step 7 is similar to the verification process [23], and the transaction is attached to the blockchain. Finally, only authorized bidders will be able to open the bidding documents and select the best bidder for the tendering agency through the prescribed processes and algorithms controlled by chaincode and MSP. The framework takes advantage of the characteristics of HLF to provide flexibility and adaptability, which can be reused in different bidding processes by introducing the required chaincode and peer.

In addition, failed bidders, managers, auditors or any other relevant parties can access the framework according to their requirements to check the quality and compliance of the

tendering process. Even anyone inside or outside the organization can monitor the process in the right time with the appropriate consent.

2.3. Smart Contract

In order to ensure privacy, Hyperledger has improved the Bitcoin architecture. On the basis of retaining the core concept of the blockchain, it provides an open-source Fabric platform. Its main contribution is the deployment of Smart Contract (SC), called chaincode in Hyperledger, which solves the problem of limited flexibility by allowing authorized participants to operate applications on the chain and reach consensus.

SC is a piece of code deployed on the blockchain and stored in the contract address, running in a specific environment, such as virtual machines, containers, etc. SC is defined by the user to write business logic, which is automatically triggered by transaction commands and invoked for execution.

Based on the openness and immutability of the blockchain, once the SC is deployed to the blockchain, any information on the SC will be transparent and cannot be modified by traditional methods. Therefore, the SC should not contain too much external logic and confidential information. If the confidential information needs to be included, then the confidential information should be encrypted before being stored in the SC. In addition, since the compilation of a complete SC involves privacy issues, security issues, legal issues, and mechanism design [24], designing an SC without security vulnerabilities, fairness, credibility, and compliance is the key issue of the system.

For bidding, a credible E-bidding process must provide a public environment that can stand the verification of participants. Based on the verifiability and non-deniability of blockchain and SC, this paper uses SC to implement the core business and simplify the bidding process.

2.4. Idemix

Identity Mixer (Idemix for short) [25] is a set of protocol encryption components developed by IBM Research. It is an anonymous credential technology based on Hyperledger [26]. Idemix can implement both strong authentication and privacy protection to hide the real identity of the client. Its two major characteristics are:

1. Anonymity, which is a function that allows transactions to be executed without revealing the identity of the trader.
2. Unlinkability, which enables multiple transactions to be sent by a single identity without showing that these transactions are issued by the same identity.

There are three roles in the Idemix process: user, issuer, and verifier. This is shown in Figure 2.

Step 1. The issuer publishes a set of user attributes in the form of a digital certificate, which is referred to as “credential” in the following.

Step 2. The user then uses the zero-knowledge proof protocol to prove that he owns the credential and selectively exposes only certain attributes contained in the credential without revealing any additional information to the verifier, the publisher, or anyone else.

Idemix technology is based on a blind signature [27,28] scheme. It supports signatures with multiple messages and valid zero-knowledge proofs in order to maximize the hiding of personal data in transactions. Therefore, Idemix is used in the E-bidding system to hide the system identity of the user and realize anonymous login.

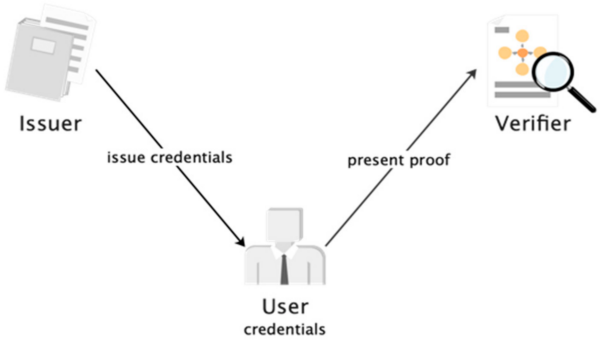


Figure 2. The roles of identity mixer.

2.5. Zero-Knowledge Proof

The concept of zero-knowledge proof (ZKP) was first proposed by Shafi Goldwasser et al. of Massachusetts Institute of Technology in the early 1980s. This paper mathematically defined the interactive ZKP systems and proposed a ZKP [29] on the judgment problem of quadratic residue.

ZKP is a kind of classical cryptography scheme that can protect privacy in multi-party interactive verification. It has been used for more than thirty years to prove the correctness of a proposition without disclosing private information. It was not until the birth of anonymous digital currency based on blockchain in recent decades that ZKP technology began to be applied on a large scale and once again became the focus of scientific research fields including fintech and big data. Therefore, if ZKP can be used in the bidding system to verify the real identity of participants, it will effectively solve many problems.

2.5.1. Graph Isomorphism

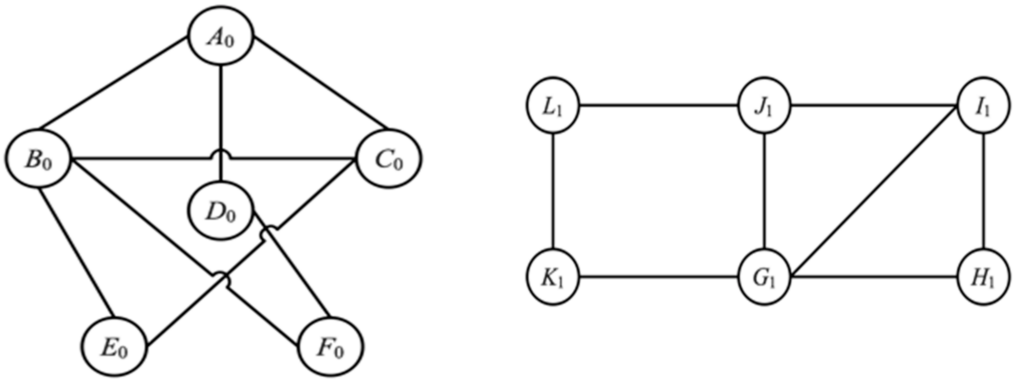
Graph isomorphism is a practical problem with very wide applications. This paper applies graph isomorphism in the field of computer science, mainly studying ZKP from the perspective of cryptography.

Definition 1. *Suppose there are two undirected (or directed) graphs, G0 and G1. If there is a bijective function* φ*:* $V(G_0) \to V(G_1)$*, such that* $\forall\ v, e \in V(G_0)$*,* $(v, e) \in E(G_0)$*, when and only when* $(\varphi(v), \varphi(e)) \in E(G_1)$*. When the multiplicity of* (v, e) *and* $(\varphi(v), \varphi(e))$ *is the same, then* G_0 *and* G_1 *are said to be isomorphic, denoted as* $G_0 \cong G_1$ [30].

It can be seen from Definition 1 that the so-called graph isomorphism is a bijection in which two graphs can completely overlap and maintain the adjacency relationship [31,32]. That is, if the nodes of a graph can be moved arbitrarily, and the edges are completely elastic, as long as one graph can be deformed into another graph without breaking, then the two graphs are isomorphic. The two graphs G_0 and G_1 in Figure 3 are isomorphic and actually represent the same graph.

2.5.2. ZKP Based on Graph Isomorphism

ZKP is mainly composed of the prover and the verifier, where the prover is generally represented by P and the verifier is represented by V. Suppose P knows that two undirected graphs G_0 and G_1 are isomorphic, and the isomorphic substitution is φ; that is, $G_1 = \varphi G_0$. P proves to V that G_0 and G_1 are isomorphic without revealing any information to V about φ; that is, V knows that G_0 and G_1 are isomorphic, but does not know how vertices correspond.



(**a**) The graph G_0 (**b**) The isomorphism graph G_1 of G_0

Figure 3. Graph G_0 and its isomorphism G_1.

The interactive ZKP protocol based on graph isomorphism is as follows [33]:

Step 1. P randomly selects a transformation π, and converts graph G_0 to graph H; that is, $H = \pi G_0$, and sends H to V.

Step 2. V randomly selects $i \in \{0, 1\}$ and sends it to P.

Step 3. P judges whether i belongs to $\{0, 1\}$, if not, then reject.

(a). If $i = 0$, record $f = \pi^{-1}$;

(b). If $i = 1$, record $f = \pi^{-1}\ \varphi$;

(c). P sends f to V.

Step 4. V Verify whether H is equal to G_i under the transformation of f; that is, $G_i = fH$ is valid. If so, accept the claim of P; otherwise, reject it.

The interactive ZKP protocol based on graph isomorphism features:

1. Completeness: Suppose P is an honest participant of the protocol and executes the protocol in strict accordance with the steps of the protocol. After repeated execution of the protocol for n times, V will accept the proof of P with a probability close to 1.
2. Soundness: In one round of this protocol, P has a $1/2$ probability of guessing V and choosing the value of i, thus cheating V. After repeated n rounds of the protocol, the probability of success of P guess is $1/2^n$, which is a small probability event. V rejects the proof of P with a probability of $1 - 1/2^n$.
3. Zero knowledge: P will generate a new graph H in each round of the protocol. After n rounds of the protocol operation, V can only gather some random isomorphic copies of graphs G_0 and G_1, and there is no information about isomorphic G_0 and G_1 between these copies. Therefore, V will not know the isomorphism of G_0 and G_1 through the protocol, so the protocol is zero-knowledge.

3. Proposed E-Bidding System

This paper proposes a double-blind E-bidding system based on blockchain. The core of the system is the use of HLF based on consortium blockchain and chaincode for business logic. The system meets the security requirements of confidentiality, immutability and anonymity. Combined with the actual bidding process, a bidding system architecture based on blockchain technology is constructed, as shown in Figure 4.

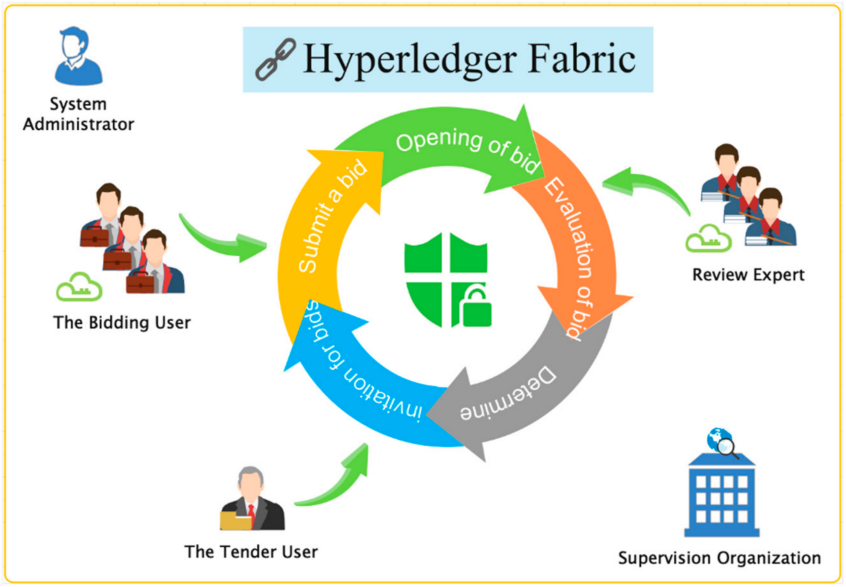


Figure 4. The architecture of blockchain-based E-bidding system.

3.1. Notation

In order to improve the reading conciseness and readability of this paper, the symbols used in the following content are listed in Tables 1 and 2.

Table 1. Description of Blockchain-based E-bidding system.

Term	Description
Admin	System Administrator
S_i	Supervisor
T_i	The Tender User
B_i	The Bidding User
E_j	Review Expert
SC	Smart Contract
GI-ZKP	ZKP Based on Graph Isomorphism

Table 2. Definition of Blockchain-based E-bidding system.

Definition	Bidding	Review
Isomorphic graph	G, $IsoGB_i$, $IsoGB_{ii}$	G, $IsoGE_j$, $IsoGE_{jj}$
Private transformation	α_i	β_j
Public transformation	ω_i	φ_j
The label	$LabelB_i$	$LabelE_j$
To construct a message	$MesB_i$	$MesE_j$
Information	$InforB_i$	$InforE_j$
Verification results of ZKP	$ResGB_i$	$ResGE_j$

3.2. System Description

Blockchain-based double-blind E-bidding system adopts consortium blockchain construction. It includes five roles: system administrator, supervisor, tenderer, bidder and review expert, and each role has several users.

1. System Administrator (*Admin*)

Admin is responsible for the management of the system, the maintenance of bidding users and review experts, and the creation of tasks for each specific bidding project.

2. Supervisor (S_i)

Review the information of bidders according to the bidding project sent by *Admin*. After passing the audit, the expert group participating in the project review will be selected.

3. The Tender User (T_i)

Send the bidding project to *Admin*, describe the project requirements and specify the bidding scoring scheme.

4. The Bidding User (B_i)

Consult the information of the bidding project, formulate the bidding document according to the project requirements, and then bid in the system.

5. Review Expert (E_j)

Accept the task of bid evaluation, review the bidding users' scheme, and score and submit the bidding scheme according to the evaluation standards of the bidding document.

3.3. GI-ZKP Verification Process

In this system, *GI-ZKP* verification is actually the authentication process, and the system can verify whether B_i or E_j is a valid user without exposing the user's information.

3.3.1. The Method of Generating Isomorphic Graph

According to the two figures G_0 and G_1 mentioned in Figure 3, the isomorphism verification is carried out as follows [32]:

The adjacency matrix of graph G_0:

$$V(G_0) = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

The adjacency matrix of graph G_1:

$$V(G_1) = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Through the program to judge whether the adjacency matrix $V(G_0)$ of G_0 can obtain the adjacency matrix $V(G_1)$ of G_1 through a finite number of elementary transformations; that is: $V(G_1) = P'V(G_0)\,P$, $P = P_1P_2 \ldots P_n$, where: P_i $(1 \leq i \leq n)$ is the elementary matrix obtained by the exchange of rows or columns of the identity matrix. By the calculation $P = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$, the bijective function φ of G_0 and G_1 is obtained: $V(G_0) \to V(G_1)$, $A \to J$, $B \to G$, $C \to I$, $D \to L$, $E \to H$, $F \to K$. Therefore, G_0 and G_1 are isomorphic, denoted as $G_0 \cong G_1$.

3.3.2. GI-ZKP Identity Authentication

When confirming participation in the bidding, the system allocates graph G to B_i, then B_i generates a unique random isomorphic transformation α_i as its private transformation. When formally bidding, B_i shall prepare the bidding plan according to the bidding

requirements and submit the bidding information $InforB_i$ (including technical solution, quotation, service, case and other information). The system uses *GI-ZKP* technology to prove the validity of bidding users. Client application generates a random isomorphic transformation ω_i, and uses B_i's private transformation α_i and public transformation ω_i to carry out compound isomorphic transformation P_i on the original image G, and obtains the verification result $ResGB_i$, then it appends the isomorphic transformation ω_i, the compound transformation P_i and $IsoGB_{ii}$ to the bidding information $InforB_i$ and sends it to the system together. That is:

1. Generate compound isomcomposition:

$$IsoGB_i = \alpha_i * G, \tag{1}$$

$$IsoGB_{ii} = \omega_i * IsoGB_i = \omega_i * \alpha_i * G, \tag{2}$$

$*$ is a matrix mapping operation.

2. Send the message $MesB_i$ to the system:

Send the message $MesB_i$: = $InforB_i$ + $LabelB_i$ + ω_i + P_i + $IsoGB_{ii}$. After receiving it, the system uses G, ω_i and P_i to verify $IsoGB_{ii}$.

3. Compare and verify whether the composite isomorphic composition generated before and after the comparison is equal:

$$P_i = \alpha_i * \omega_i, \tag{3}$$

$$ResGB_i = P_i * G, \tag{4}$$

$$ResGB_{ii} = IsoGB_{ii}? \text{ User is valid: User is invalid.} \tag{5}$$

If it is match, it indicates that B_i can prove that it is a valid user under the condition of concealing private transformation α_i. So as to avoid malpractice in the bidding process caused by the disclosure of B_i identity information. The validation process is shown in Figure 5.

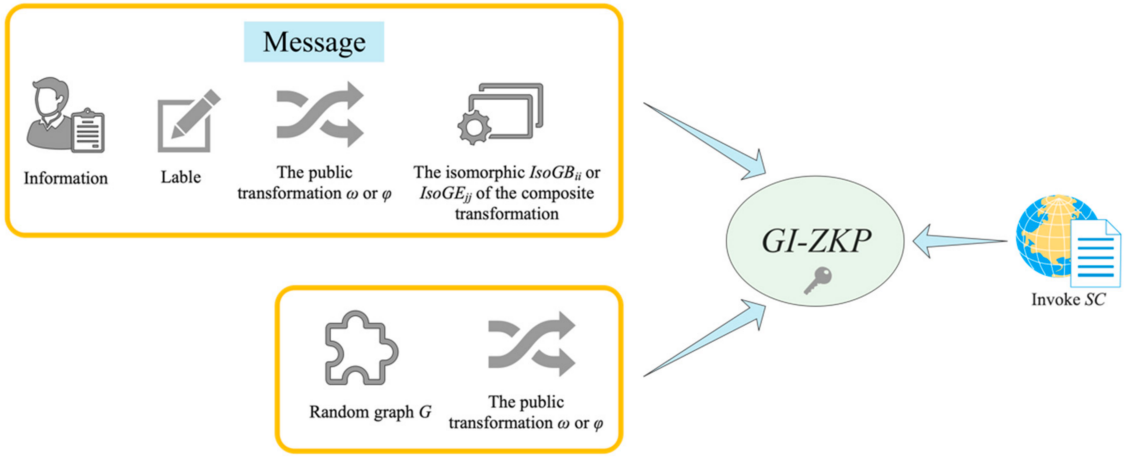


Figure 5. *GI-ZKP* identity authentication.

E_j is also required to demonstrate its legitimacy to the system using *GI-ZKP* technology prior to the formal review. The process is the same as the bidding process, as shown in Figure 5.

3.4. Processes and Steps

The E-bidding system based on the consortium blockchain described in this paper is built on the HLF platform. Idemix and ZKP technologies are enabled to realize the

anonymous login of users. The tendering and bidding process includes three stages: initial preparation stage, bidding stage and review stage. In the bidding stage and the review stage, the *GI-ZKP* method is used to protect user privacy, which not only hides the identity information of bidding users and review experts, but also ensures the authenticity of user identity. It can effectively resist the attack mode of malicious users inferring expert identity through data analysis, and also guarantee the anonymity of bidding users.

The overall process of the system is shown in Figure 6.

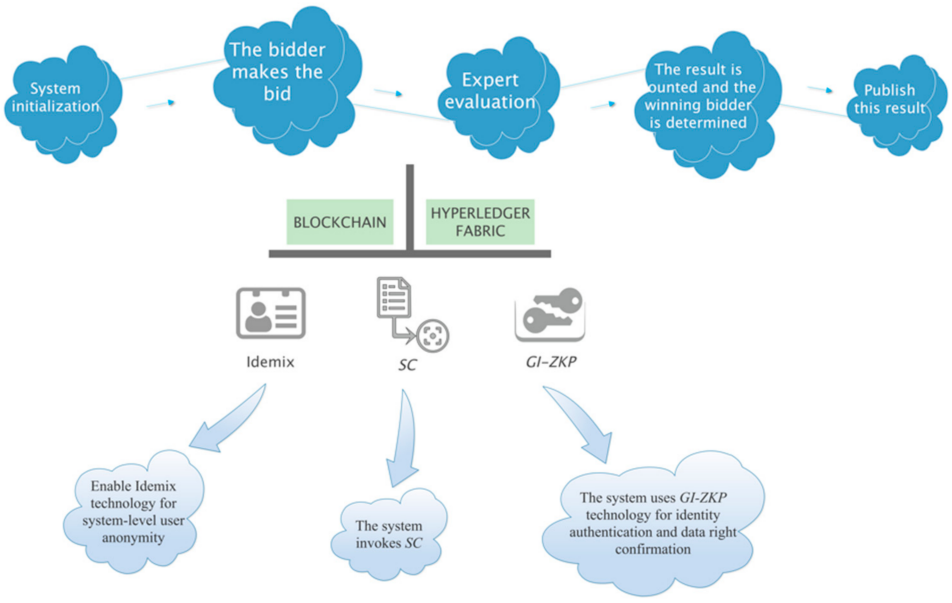


Figure 6. System workflow.

3.4.1. The Initial Preparation Stage

Admin generates a label randomly for both B_i and E_j, respectively, records the label into the label list after hash operation, and sends the label under the corresponding user.

B_i selects a private transformation α_i on the basis of the graph G and keeps the transformation secret. This transformation is used to generate an isomorphic $IsoGB_i$ of G; that is: $IsoGB_i = \alpha_i * G$.

E_j selects a private transformation β_j on the basis of the graph G and keeps the transformation secret. This transformation is used to generate an isomorphic $IsoGE_j$ of G; that is: $IsoGE_j = \beta_j * G$.

3.4.2. The Bidding Stage

B_i selects a public transformation ω_i based on the first transformation to generate isomorphic graph $IsoGB_i$, which uses this transformation to generate $IsoGB_i$ isomorphic diagram $IsoGB_{ii}$; that is: $IsoGB_{ii} = \omega_i * IsoGB_i = \omega_i * \alpha_i * G$.

Construct a message $MesB_i$: $= InforB_i + LabelB_i + \omega_i + IsoGB_{ii}$; the bid information $InforB_i$ does not contain B_i's identity information. Record $LabelB_i$ to the label list and submit $MesB_i$ to the system.

After receiving the message $MesB_i$ sent by B_i, *Admin* invokes *SC* and uses *GI-ZKP* to verify whether the B_i identity is a valid bidder, as shown in Figure 5. The generated validation result $ResGB_i$ is compared with the previously generated $IsoGB_{ii}$. If it is the same and $LabelB_i$ is only in the label list, but not in the consumed label list, it is a valid B_i.

After B_i identity authentication is successful, $LabelB_i$ will be sent to the list of consumed label. In addition, $InforB_i$, $IsoGB_{ii}$ and ω_i will be recorded, and the bidding information will be made public.

3.4.3. The Review Stage

B_i selects a public transformation φ_j based on the first transformation to generate isomorphic graph $IsoGE_j$, which uses this transformation to generate $IsoGE_j$ isomorphic diagram $IsoGE_{jj}$; that is: $IsoGE_{jj} = \varphi_j * IsoGE_j = \varphi_j * \beta_j * G$.

Construct a message $MesE_j$: = $InforE_j$ + $LabelE_j$ + φ_j + $IsoGE_{jj}$; the review information $InforE_j$ does not contain E_j's identity information. Record $LabelE_j$ to the label list and submit $MesE_j$ to the system.

After receiving the message $MesE_j$ sent by E_j, *Admin* invokes *SC* and uses *GI-ZKP* to verify that the E_j is a valid review expert, as shown in Figure 5. The generated validation result $ResGE_j$ is compared with the previously generated $IsoGE_{jj}$. If it is the same and $LabelE_j$ is only in the label list but not in the consumed label list, it is a valid E_j.

After E_j identity authentication is successful, $LabelE_j$ will be sent to the list of consumed label. Furthermore, $InforE_j$, $IsoGE_{jj}$ and φ_j will be recorded, and the review information will be made public. If the amount of review information received is equal to the number of review experts, the review results shall be counted to determine the bid winner. Finally, all review information is made public together.

3.5. Problem Analysis

1. Access to information

Any authorized participants can invoke the *SC* to check the tender, bidding and review information. However, the public information hides their real identity information through ZKP and other privacy mechanisms. Instead, private transformation, public transformation, isomorphic graph generated by multiple transformations of random graph G and unique label are used to represent their identities. Therefore, except for the main body who released the information, the rest of the people could not know the association between the bidding information and B_i, or the association between the evaluation opinions and E_j.

2. Data ownership confirmation

After the bidding or review, in order to prevent information tampering and disclosure, the system still uses *GI-ZKP* technology to confirm the ownership of the information submitted by B_i or E_j. The user uses the corresponding private transformation α_i or β_j and the public transformation ω_i or φ_j returned by the system to verify the compound isomorphism of the original graph G. The result $ResGB_i$ or $ResGE_j$ of ZKP validation is compared with the previously generated compound isomorphism graph $IsoGB_{ii}$ or $IsoGE_{jj}$. If the two graphs are the same, it indicates that the information was actually posted by the user.

3. Duplicate submissions preventing

For both B_i and E_j, it is necessary to prevent them from submitting bidding information and review information repeatedly, otherwise it will lead to system disruption. When the system receives the bidding information of B_i or the review information of E_j, it shall check whether the hash value of the label carried has been included in the list of issued labels. If not, it is proved to be the information submitted by an invalid user and can be ignored. If it is, check whether the hash value of the label is in the consumed label list. If it is still in the consumed label list, it indicates that it is a duplicate submission and will be rejected.

4. Experimental Settings

In order to verifying the system, we setup an HLF platform and deployed our application in the experimental environment.

4.1. Hardware/Software

- PC: five PCs;
- Processor: 2.4-GHz Intel Core i5;
- Memory: 4-GB 1600-MHz DDR3;

- Docker Fabric Cluster: Centos7.2, 16G, E2500;
- Web applications: Spring MVC architecture;
- Client Operating system: MacOS Mojave 10.14.6;
- SC code: Go 1.14.2.

4.2. Operating Procedures

4.2.1. The Initial Preparation Stage

1. T_i logs into the system to issue the tender application;
2. S_i of the Authority shall verify whether the tendering unit meets the tendering qualification.

4.2.2. The Bidding Stage

1. After B_i sees the project available for bidding in the message board, it will issue a bid application and fill in the company's business scale, etc.;
2. S_i verifies whether the bidding company is qualified to bid. The system randomly allocates graph G and unique string $LabelB_i$ for the bidding project to be bid, and sends them to the qualified B_i;
3. B_i shall download the tender after qualification and bid after the design scheme. At this time, B_i needs to invoke SC and prove its authenticity to the system with ZKP technology.

4.2.3. The Review Stage

1. After B_i applies for bid opening, S_i generates the bid review team. The review team obtains the original drawing G and unique strings of the $LabelE_j$ randomly allocated by the system according to the bidding scheme, and sends them to qualified E_j;
2. The bid review team shall review the bids according to the bid review tasks. At this time, E_j needs to invoke SC and use ZKP technology to prove its authenticity to the system;
3. T_i selects the winning bidder based on the review results of the review team and closes the bidding.

4.3. Smart Contract

In this experiment, the chaincode based on HLF is run in a secure and lightweight docker, and the SC for chaincode is written with Go language. The normal operation of chaincode requires state retrieval and interaction with the world state database.

Before bidding formally, the system uses *GI-ZKP* technology to authenticate the identity of bidding users. The previously generated composite isomorphic graph *IsoGB*2 is compared with the now generated composite validation result *ResGB*2, and if they are the same, it is proved that the bidder is a real user. The same goes for reviews. The pseudocode of the proposed scheme (Algorithm 1) is shown below.

4.4. Experimental Results

By adopting SC and *GI-ZKP* technology, the system can not only confirm the legitimacy of B_i and E_j, but also prevent the leakage of B_i and E_j information. As a result, the function of verifying whether the other party is valid B_i and E_j under the premise of concealing the real identity of the user is realized. This avoids unfair review caused by B_i contacting E_j before bid opening.

All the information of each link of bidding is recorded on the blockchain, and only one submission is allowed, so as to achieve the effect of information disclosure, traceability, and non-tampering. This ensures the integrity and fairness of bidding information, and effectively guarantees the smooth development of E-bidding activities.

Algorithm 1 Zero-Knowledge Proof.

Input: BMes
Output: True or False

```
01:  if fcn == "ZKP" {
02:  var bmes BMes
03:  bInfor := bmes.BInfor
04:  bID := bmes.BID
05:  blabel := bmes.BLabel
06:  t2 := bmes.BT2
07:  IsoGB2 := bmes.BG2
08:  //The system authenticates the identity if the label unique validation is satisfied.
09:  if cc.hasLable(stub, bID, blabel) && !cc.isConsumer(stub, bID, blabel) {
10:  //Gets a random graph G0.
11:  key, err := stub.CreateCompositeKey("BG0", []string{bID, blabel})
12:  if err != nil {
13:  return shim.Error(err.Error())
14:  }
15:  getg0, err := stub.GetState(key)
16:  var g0 [][]int
17:  json.Unmarshal(getg0, &g0)
18:  //Gets the first mapping mode T1.
19:  key, err = stub.CreateCompositeKey("BT1", []string{bID, blabel})
20:  gett1, err := stub.GetState(key)
21:  var t1 []int
22:  json.Unmarshal(gett1, &t1)
23:  //When ZKP is verified, the compound transform isomorphic ResGB2 is obtained.
24:  ResGB1 := cc.getG1(g0, t1)
25:  ResGB2 := cc.getG2(g11, t2)
26:  IsoGB, err := json.Marshal(IsoGB2)
27:  ResGB, err := json.Marshal(ResGB2)
28:  //Compare whether the isomorphic graphs IsoGB2 and ResGB2 after two composite
     transformations are equal to verify the authenticity of the user.
29:  if string(IsoGB) == string(ResGB) {
30:  return shim.Success([]byte("true"))
31:  }
32:  }
33:  }
```

5. Safety Analysis

An excellent E-bidding system requires several key factors to balance. The security of the E-bidding system is analyzed from the following three aspects below. The security of the system is mainly based on the blockchain technology and the ZKP protocol.

5.1. Privacy Security

In a double-blind public E-bidding system, Idemix technology provided by Hyperledger is enabled to achieve system-level user anonymity. On this basis, platform level anonymity is realized by using the ZKP mechanism based on blockchain. Both of them conceal the real identity information of the user, thereby avoiding privacy leakage in the process of data interaction, and also preventing the use of data analysis to infer the identity of the user.

In addition, the system replaces the traditional database with SC based on blockchain technology. Nodes on the blockchain network participate in verification and calculation, which not only increases the anonymity of users but also guarantees the security of data transmission and improves the credibility and verifiability of the open phase. This effec-

tively improves and makes up for the defects and risks of the system in terms of data privacy and information security.

5.2. Energy Saving and High Efficiency

The HLF-based framework allows different types of peer nodes to manage individual chaincodes through channels. Moreover, only a few trusted nodes are sufficient to process the same transaction without having to wait for each node. As a result, the transaction speed is accelerated and can be expanded as needed [23]. In addition, the traditional mining process is not required, thus saving time and money.

When a problem is encountered, the traditional mechanism requires a lot of processing time; on the contrary, the SC of the blockchain can implement complex business logic, such as quickly extracting the entire bidding information, but without or with less manual intervention [34]. At the same time, it has also greatly reduced the waste of resources and effectively reduced transaction costs, thereby ensuring that the bidding activities are more energy-efficient and efficient.

5.3. Fairness and Credibility

Different from ordinary tendering and bidding activities, E-bidding is not only subject to the real-time supervision and constraints of the industry regulatory authorities, but also subject to the supervision of the public, which reduces the occurrence of bad credit problems and effectively avoids illegal bidding, together-conspired bidding and contacting bid, thus creating a fair and benign competitive environment in the bidding market [35].

In the E-bidding system, once all bidding information is submitted to the system, all the bidding information will be stored on the chain to ensure the full transparency and traceability of the bidding process. Therefore, all the materials are authentic and effective, immediately available, and cannot be tampered with and forged, which improves the credibility of bidding information.

6. Conclusions

This paper proposes the design and implementation method of a distributed E-bidding system based on blockchain. Its core idea is to combine blockchain technology with privacy protection, so that all participants using this system can safely participate in the opening stage. Different from the current E-bidding system, this system still uses a trusted third party, replacing it with an SC with public and transparent attributes. SC is used to store records and check information during the bidding process.

At the same time, this paper uses a "Permissioned Blockchain" such as Hyperledger to develop the bidding process. Among them, chaincode and MSP can control the access of a single user together and can also set a time limit for it. Therefore, the risk of distributed denial of service (DDoS) attacks entering the network is greatly reduced, thereby ensuring the extensive security, confidentiality and non-repudiation of the entire process.

Although the system has solved many shortcomings in the existing system, there are still some limitations and challenges in the implementation. The details are as follows:

1. HLF is a very new technology with rapidly changing functions. Establishing such a new network and getting other stakeholders to adapt to it is a huge challenge.
2. Compared with other E-bidding systems, this system requires more time and computing resources. After 50 experiments, the system takes an extra 2.3 s on average after adding the privacy protection mechanism. Among them, the highest extra cost is 3.6 s, and the lowest extra cost is 1.2 s. Therefore, there is a trade-off between resource consumption and security performance in this case.
3. The lack of skilled blockchain technical personnel to operate and maintain the system is also an obstacle.

For now, this system has significant advantages different from other E-bidding systems and has a longer-term development prospect. In the future, in-depth research can be conducted from the following two aspects:

1. Adding other privacy protection mechanisms to the bidding system, such as blind signature [36] and secure multi-party calculation [37], etc., can make the bidding process more fair and secure.
2. Secondly, the framework will not be limited to the field of bidding but will also be explored in other enterprise blockchain services, such as insurance, human resources, healthcare and more similar infrastructure.

To sum up, the fundamental purpose of this paper is to provide a technical solution to make the participants' privacy information in the E-bidding system more secure and the bidding environment more reliable. Therefore, relevant organizations should identify opportunities, vigorously develop E-bidding systems, absorb advanced technologies and management concepts, keep up with the pace of the times, and promote the sustainable development of the industry.

7. Patents

There is a patent resulting from the work reported in this manuscript, which is in opening status and can be queried from https://www.cnipa.gov.cn/. The patent ID is 202010441768.8, and the access date is 3 August 2020.

Author Contributions: D.W., J.Z. and C.M. developed the idea, protocol design, and wrote the original draft. D.W. improved the scheme, provided useful advice, and performed the experiment. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Shandong Provincial Natural Science Foundation, China, grant number ZR2020MF148.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wang, B.C.; Sun, J.W.; He, Y.H.; Pang, D.D.; Lu, N.X. Large-scale Election Based on Blockchain. *Procedia Comput. Sci.* **2018**, *129*, 234–237. [CrossRef]
2. Abuidris, Y.; Kumar, R.; Wang, W.Y. *A Survey of Blockchain Based on E-Voting Systems*; ICBTA; Association for Computing Machinery: New York, NY, USA, 2019; pp. 99–104.
3. Kshetri, N.; Voas, J. Blockchain-Enabled E-Voting. *IEEE Softw.* **2018**, *35*, 95–99. [CrossRef]
4. Andrew, B.; Christopher, B.; Thomas, P. Digital Voting with the Use of Blockchain Technology. Available online: https://www.economist.com/sites/default/files/plymouth.pdf (accessed on 18 December 2018).
5. Fan, C.I.; Wu, C.N.; Sun, W.Z. Multi-recastable E-Bidding Scheme. In Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications, Kaohsiung, China, 26–28 November 2008; pp. 462–466.
6. Xu, J.; Song, J.R. A New Management System for Intelligent E-Bidding. In Proceedings of the IEEE 4th International Conference on Software Engineering and Service Science, Beijing, China, 23–25 May 2013; pp. 158–161.
7. Rinh, V.A.; Trinh, V.C. One-Verifier Signature Scheme and Its Applications. In Proceedings of the Tenth International Symposium on Information and Communication Technology, Hanoi Ha Long Bay, Vietnam, 4–6 December 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 261–266.
8. Tang, J. The Application of Ethereum Smart Contract Technology in Bidding Review of Construction Projects. *Constr. Archit.* **2020**, *21*, 70–73.
9. Hardwick, F.S.; Akram, R.N.; Markantonakis, K. Fair and Transparent Blockchain Based Tendering Framework—A Step towards Open Governance. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1342–1347.
10. Galal, H.S.; Youssef, A.M. Succinctly Verifiable Sealed-Bid Auction Smart Contract. In Proceedings of the ESORICS 2018 International Workshops (DPM 2018 and CBT 2018), Barcelona, Spain, 6–7 September 2018; Springer: Cham, Switzerland, 2018; pp. 3–19.
11. Manimaran, P.; Dhanalakshmi, R. Blockchain-Based Smart Contract for E-Bidding System. In Proceedings of the 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), Jaipur, India, 28–29 September 2019; pp. 55–59.
12. Blass, E.O.; Kerschbaum, F. BOREALIS: Building Block for Sealed Bid Auctions on Blockchains. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20), Taipei, Taiwan, 1–5 June 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 558–571.

13. Li, X.C. BCES: A BlockChain based Credible E-Bidding System. In Proceedings of the 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 11–14 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 2415–2421.
14. Sarfaraz, A.; Chakrabortty, R.K.; Essam, D.L. A Tree Structure-Based Improved Blockchain Framework for a Secure Online Bidding System. *Comput. Secur.* **2021**, *102*, 102147. [CrossRef]
15. Omar, I.; Hasan, H.; Jayaraman, R.; Salah, K.; Omar, M. Implementing Decentralized Auctions Using Blockchain Smart Contracts. *Technol. Forecast. Soc. Chang.* **2021**, *168*, 120786. [CrossRef]
16. Tso, R.; Liu, Z.Y.; Hsiao, J.H. Distributed E-Voting and E-Bidding Systems Based on Smart Contract. *Electronics* **2019**, *8*, 422. [CrossRef]
17. Wang, D.; Zhao, J.D.; Wang, Y.J. A Survey on Privacy Protection of Blockchain: The Technology and Application. *IEEE Access* **2020**, *8*, 108766–108781. [CrossRef]
18. Wang, Z.J. Application Practice of Blockchain Technology in Bidding Field. *China CIO News* **2020**, *8*, 96–97.
19. Hyperledger Whitepaper. Available online: http://www.8btc.com/hyperledger-whitepaper (accessed on 18 July 2016).
20. Suciu, G.; Nădrag, C.; Istrate, C.; Vulpe, A.; Ditu, M.C.; Subea, O. Comparative Analysis of Distributed Ledger Technologies. In Proceedings of the 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 370–373.
21. Nawari, N.; Nawari, S. Blockchain technology and BIM process: Review and potential applications. *ITcon* **2019**, *24*, 209–238.
22. Zou, X.Q.; Luo, D.C.; Lin, P.; Shen, S.P.; Xie, Z.P.; Wang, Y.J.; Ding, Y. System of River Chief-Oriented Water Quality Information Certification Based on Blockchain. *J. Appl. Sci.* **2020**, *38*, 65–80.
23. Mustafa, M.K.; Waheed, S. A governance framework with permissioned blockchain for the transparency in e-tendering process. *IJATEE* **2019**, *6*, 61. [CrossRef]
24. OuYang, Y.L.; Wang, S.; Yuan, Y.; Ni, C.X.; Wang, F.Y. Smart Contracts: Architecture and Research Progresses. *Acta Autom. Sin.* **2019**, *45*, 445–457.
25. Camenisch, J.; Herreweghen, E.V. Design and Implementation of the Idemix Anonymous Credential System. In Proceedings of the ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002; Association for Computing Machinery: New York, NY, USA, 2003; pp. 21–30.
26. Idemix in Hyperledger Fabric. Available online: https://zhuanlan.zhihu.com/p/41265144 (accessed on 4 August 2018).
27. Shao, Q.; Hong, H.J.; Li, B. Research on Blockchain Electronic Voting Scheme Based on Elgamal Strong Blind Signature. *J. Chin. Comput. Syst.* **2021**, in press.
28. Dong, Y.K. Design and Implementation of Blockchain-Based Security E-Voting System. Master's Thesis, Beijing Jiaotong University, Beijing, China, 2019.
29. Goldwasser, S.; Micali, S.; Rackoff, C. The knowledge complexity of interactive proof systems. *SIAM J. Comput.* **1989**, *18*, 186–208. [CrossRef]
30. Hou, A.M. Theory Research and Algorithm Design on Hamiltonian Cycle and Graph Isomorphism Problems. Ph.D. Thesis, South China University of Technology, Guangzhou, China, 2013.
31. Francisco, M.F.; Pino, C.G.; Cándido, C.G. Authentication Based on Non-Interactive Zero-Knowledge Proofs for the Internet of Things. *Sensors* **2016**, *16*, 1.
32. Li, Y.L.; ShangGuan, J.T.; Jia, J. A Zero-Knowledge Proof Protocol Based Graph Isomorphism Algorithm. *J. North Univ. China* **2014**, *35*, 299–302, 308. [CrossRef]
33. Zhu, H.W. The Research Based on the Zero Knowledge Discusses About the Graph Questions and the Network Security. Master's Thesis, Chengdu University of Technology, Chengdu, China, 2007.
34. The Application Research of Electronic Bidding System Based on Blockchain Technology. Available online: http://www.entrepreneurdaily.cn/2020-06-01/3/2389858.html (accessed on 1 June 2020).
35. Li, F. The Application of Blockchain in the Performance Management of Bidding Market. *China Tendering Wkly.* **2018**, *30*, 13–15.
36. Chaum, D. Blind Signatures for Untraceable Payments. In *Advances in Cryptology*; Springer: Boston, MA, USA, 1983; pp. 199–203.
37. Wang, T. A Review of the Study of Secure Multi-party Computation. *Cyberspace Secur.* **2014**, *5*, 41–44.