Blockchain based Smart Contract for Bidding System

Yi-Hui Chen
Department of M-Commerce and Multimedia Applications,
Asia University,
No. 500, Lioufeng Rd., Wufeng Dist., Taichung City 41354, Taiwan
Email: chenyh@asia.edu.tw

Shih-Hsin Chen*
Department of Information Management,
Cheng Shiu University,
No.840, Chengcing Rd., Niaosong Dist., Kaohsiung City 83347, Taiwan
Email: shchen@csu.edu.tw
(Correspondence author: Shih-Hsin Chen)

Iuon-Chang Lin
Department of Management Information Systems,
National Chung Hsing University,
145 Xingda Rd., South Dist., Taichung City 402, Taiwan
Email: iclin@nchu.edu.tw

Abstract

Because of the popularity of the Internet, the integration services have gradually changed people daily life, such as e-commerce activities on transactions, transportation and so on. The E-auction, one of the popular e-commerce activities, allows bidders to directly bid the products over the Internet. As for sealed bid, the extra transaction cost is required for the intermediaries because the third-party is the important role between the buyers and the sellers help to trade both during the auction. In addition, it never guarantees whether the third-party is trust. To resolve the problems, the blockchain technology with low transaction cost is used to develop the smart contract of public bid and sealed bid. The smart contract, proposed in 1990 and implements via Ethereum platform, can ensure the bill secure, private, non-reputability and inalterability owing to all the transactions are recorded in the same but decentralized ledgers. The smart contract is composed of the address of Auctioneer, the start auction time, deadline, the address of current winner, the current highest price. In the experiments, the accounts are created through Ethereum wallet. In miner stage, the MinerGate is used in miner stage for obtaining money to pay the transaction fee. At recorder stage, the nodes of blockchain are synchronized to generate smart contract.

Keywords: E-auction, Public Bid, Sealed Bid, Blockchain, Smart Contract

Introduction

In recent years, E-auction [1, 3, 9, 10, 11, 13] is the popular issue since its convenience and efficiency. E-auction integrates the network technique into the bidding system in order to reduce the cost of transactions. The main roles during E-auction include bidders, auctioneers, and the third-party as shown in Fig. 1. Most of the third party is the centralized intermediary to provide a platform to help bidders and auctioneers posting products, checking the highest bidding price and committing the winner, such as eBay and yahoo bidding system. However, E-auction has two main problems. First, a centralized intermediary is required in bidding system to help communication between bidders and auctioneers. The charge fees for the centralized intermediary to increase the transaction cost. Besides, the personal data and transaction records are stored in database might cause privacy leakage. Secondly, in a sealed envelope [8], bidders have no way to ensure that lead bidder never leaks their bidding price.

Fig. 1: The role of the E-auction

This paper applies the blockchain technique into the E-auction to resolve the two problems. The blockchain [5, 6, 14] is peer-to-peer access structure such that points in the structure can trust each other points. Each location can securely communicate, authenticate and transfer data to any of the other sites. Consequently, in the decentralized structure, the centralized intermediary can be removed to reduce the transaction cost [7, 15]. As for the second problem, the smart contract is used to avoid the bid price leaked by the lead bidder. Some rules are written inside the smart deal which can not be opened before the deadline.

This paper is organized as follows. Section 2 reviews the traditional bidding system and the blockchain. Section 3 shows how do we integrate the blockchain technique into the bidding system. In order to validate the proposed method, we conduct the experiments in Section 4 and we draw our conclusions in

ISBN 978-1-5386-4342-6

Section 5.

Related Works

A. Traditional Bidding System

Nowadays, E-auction can be classified into two types, namely public bid and sealed bid [2]. Public bid is that bidders could raise the price to bid the products. Thus, the bidding price gets increasing continuously until no bidders are willing to pay a higher price. The bidder is as a winner if he bids the highest price for such the product. During public bid, bidders can bid several times; thus, public bid is also called multi-bidding auction. Sealed bid is that bidders encrypts the bill and only send the bill once. If the time is due, the auctioneer compares all of the bills. The bidder who bids for the highest price is the winner of the sealed bid. Due to bidders only can bid once, it is also called single-bidding auction. In the seal bid, all bidders' prices are sealed until the bid opening deadline is compared to the prices of all bidders. There is a common shortcoming in electronic seal ticket auctions. Before the deadline for opening bids, the bidder cannot ensure that the bid price has been leaked by a third party (the principal bidder), resulting in malicious bidders may collaborate with the bid winner to obtain the best bid price.

B. Blockchain

The blockchain [5, 6, 14] is a technology that accesses, verifies, and transmits network data through distributed nodes. It uses a peer-to-peer network to achieve a decentralized data operation and preservation platform. The blockchain is mainly based on the following technologies as the operating base:

(1) Identity identification and security: Identification and anti-counterfeiting are performed using a public key infrastructure. Each account in the blockchain has a public key and a private key used to send and receive the transactions. After the private key encrypts the transaction message, the receiver then uses the sender's public key to decrypt the message, and the identity of the sender can be confirmed.

(2) Message delivery and broadcasting: Message delivery and broadcasting are performed using a peer-to-peer technique, allowing each node to connect and exchange messages with each other. The transactions are stored in the same ledger. Each node in the blockchain can verify the transactions using the zero knowledge over the decentralized access structure.

(3) Data preservation and linking: The transaction data stored in a block to generate a hash value and the block is linked to the previous block with the hash values to construct a blockchain as shown in Fig. 2. The fields in the block, as shown in Fig. 3, to detail the records of the block such as time-stamp, transaction quantity, hash value, etc.

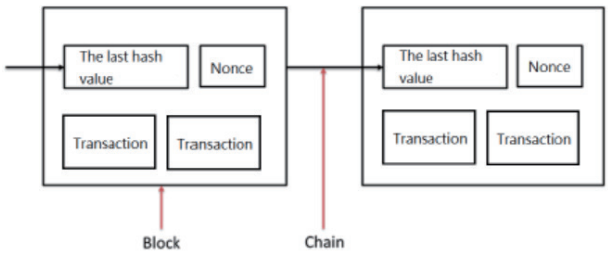

Fig. 2: The relationship between the block and chain

field	data
Number Of Transactions	1750
Transaction Fees	0.7211382 BTC
Height	443666 (Main Chain)
Timestamp	2016-12-16 04:58:11
Difficulty	310,153,855,703.43
Bits	402885509
Size	998.306 KB
Block Reward	12.5 BTC
Hash	000000000000000000bc00a7082f0805ba882d1dabac3dd0562ba6162e93a082
Previous Block	000000000000000003231d0dbad32b1f3219af0eeb16289d907c2d7b86b68524
Next Block(s)	000000000000000004a6f37e94a28076ce4e0f6965869c47e0f60c3abf21e0f
Merkle Root	c003190d380153505850c589dddf7bff46dc1420a871de81c002e5bc1a2b46c5

Fig. 3: The field names of each block

In the blockchain, there might be different transactions in a block. When a new transaction is just triggered, each node collects unverified transactions to the block to produce a POW (Proof of Work). That is, the node can calculate the Nonce to verify the transaction as soon as possible to get some rewards. If the node completes the proof of work, it broadcast the block to other nodes to verify whether the transaction is valid. If valid, the block is attached to the blockchain.

Research Method

The flowchart of E-auction is shown in Fig. 4, the seller post the bidding information including product description and starting price at the first stage. Bidders vote the sealed envelope to bid the product with a higher price. After receiving the sealed envelope, the auctioneer announces the highest rate right now. The bidder is as the winner bidder until no one bid the product with the higher price or the deadline is due. The auctioneer can get the money from winner and send the product to the bidder. We develop an open bidding system through blockchain with smart contracts. Bidders write the trade contract for the bids into the blockchain. With decentralized access structure, all bidders can bid the product by calling the open contract's trading contract without intermediate brokers.

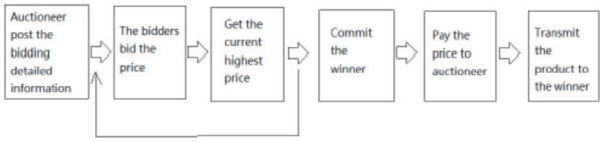

Fig. 4: The flowchart of E-auction

A complete public E-auction system must satisfy the following requirements:

(1) The identity of the person who is a bidder or winner (successful bidder) is anonymous to everyone.

(2) During a transaction, the content of seal order cannot be modified, and all the people can verify whether its correctness and completeness.

(3) No illegal bidder can impersonate the legal one to bid the product. After bidding, no one can deny the bidding if they have ever bidded.

(4) The successful bidder always has the proof to get the product.

(5) The seller can get the money from the successful bidder but not for the other bidder.

ISBN 978-1-5386-4342-6

(6) The sealed envelope must be delivered before the deadline; otherwise, the envelope is invalid.
(7) Before the deadline, the sealed envelope is private, and no one can open it.
(8) A fair solution is required if the same price is voted by two different bidders.

The smart contract [4, 12] is a set of codes and digits implemented via Ethereum platform. In an intelligent agreement, the contract is started if the time or event is triggered, such as sending a message, dealing with transactions, terminating the contract. The smart contract is described by Solidity, Serpent, LLL, and EtherScript. The Solidity is the way we used in this article. The bytecode of smart contract retrieved with JSON format is used for broadcasting all the nodes of blockchain and wait for verifying. If true, the smart contract is announced with individual contract address and JSON Interface to allow the other person to join in. Over Ethereum Wallet, we use Watch Contract to invite other people to join. Before the deadline, all the legal bidders can send the sealed envelope to renew the price. All the sealed envelopes are opened when the time is due. The highest price on the sealed envelope is the final winner.

In the initialization data, we will announce the following information in advance.

(1) Auctioner: The tenderer address used to record the originating contract.
(2) AuctionStart: Used to announce the start time of the bid.
(3) biddingTime: Used to announce the effective time of the contract.
(4) highestBidder: The address of the bidder who currently bids the product with the highest price.
(5) highestBid: Used to record the current highest price.

As for the contract, we define the following function:

(1) blindAuction(): Activate the contract by calling this function, and use the auctionStart and biddingEnd to record the start and end time.
(2) Bid(): This function can be called by any person to perform the bidding action. Before the function is executed, AuctionStart and biddingTime are used to judge whether the contract is expired. If not, the bidder can send the bid envelope if the price is greater than the current highest price. The contract system will use highestBid and highestBidder to record the current highest price and the corresponding bidder's address.
(3) reveal(): Opens the bid by calling this function, and compares the prices of all the tickets to get the final winner.
(4) AuctionEnd(): In this function, AuctionStart and biddingTime are automatically used to determine the contract validity time. If the effective time ends, the successful bidder's Address and the current highest price will be automatically sent to the tenderer. This function will be disabled to avoid repeated execution.
(5) withdraw(): Returns the amount of bids tendered by bidders other than the successful bidder.

Empirical Results

In the experiments, we create two blockchain accounts using Ethereum Wallet for testing and bidding transactions. In the miner, we adopt command-line and MinerGate to execute the data miner to get the coin for paying the transaction fee as shown. We can use the command-line to check the transaction status for the details of blocks in blockchain as shown in Fig. 6. In smart contract creation, three stages, namely writing, compiling, and announcing by using Solidity programming. The bytecode is generated by Solidity realtime compiler. The Solidity runtime is used to generate the Interface as shwon in Fig. 5. Finally, we can use Ethereum Wallet to announce the smart contract to the blockchain as shown in Fig. 7. During the testing phase, the smart contract is verified to get the address of the contract. The second account can add the new bidding to the contract by using Solidity and Interface.

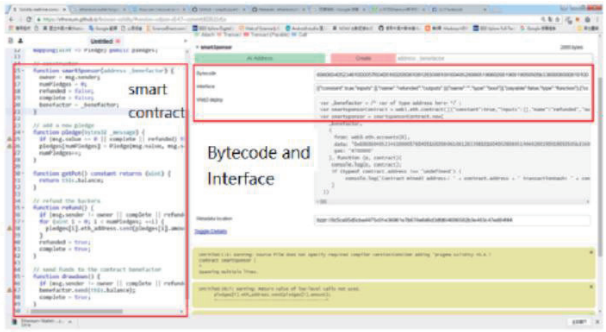

Fig. 5: The smart contract and its corresponding bytecode and interface

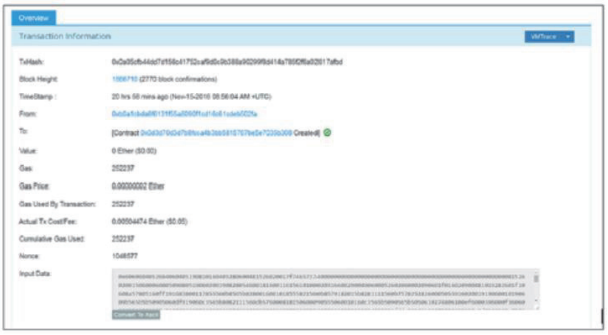

Fig. 6: The details of smart contract

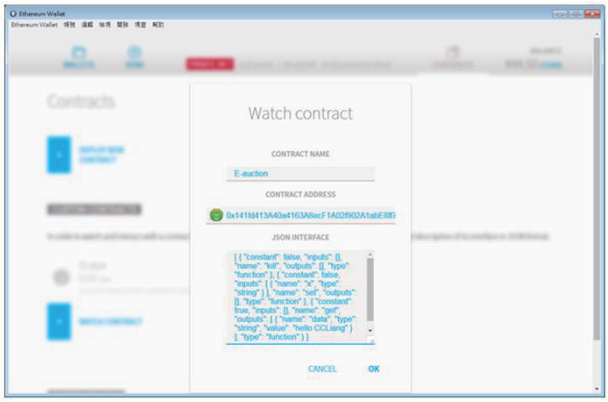

Fig. 7: Smart contract announcement

Conclusions

This paper provides an E-auction mechanism based on

ISBN 978-1-5386-4342-6

blockchain to ensure electronic seals confidentiality, non-repudiation, and unchangeability. We expect to encounter potential problems in the implementation of this work. In smart contracts for sealed orders, due to the complexity of the contract, the bidders and bidders come, say may call the wrong contract function. For example, the bidder inadvertently calls Reveal() to open all bids, so that the bidding must be terminated and re-arranged. For this purpose, we will set the authority judgment for different functions and will perform the function before first determine if the caller can perform this function.

Acknowledgment
We thank the Ministry of Science and Technology for supporting this research with IDs MOST 106-2221-E-230-009 and MOST 106-2221-E-468-001 and MOST 105-2410-H-005-023-MY2.

References

[1] Gang Cao and Jie Chen. Practical electronic auction scheme based on untrusted third-party. In *Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on*, pages 493–496. IEEE, 2013.

[2] llichetty S Chandrashekar, Y Narahari, Charles H Rosa, Devadatta M Kulkarni, Jeffrey D Tew, and Pankaj Dayama. Auction-based mechanisms for electronic procurement. *IEEE Transactions on Automation Science and Engineering*, 4(3):297–321, 2007.

[3] Wen Chen and Feiyu Lei. A simple efficient electronic auction scheme. In *Parallel and Distributed Computing, Applications and Technologies, 2007. PDCAT'07. Eighth International Conference on*, pages 173–174. IEEE, 2007.

[4] Christopher K Frantz and Mariusz Nowostawski. From institutions to code: Towards automated generation of smart contracts. In *Foundations and Applications of Self* Systems, IEEE International Workshops on*, pages 210–215. IEEE, 2016.

[5] Marco Iansiti and Karim R Lakhani. The truth about blockchain. *Harvard Business Review*, 95(1):118–127, 2017.

[6] M Jenifer and B Bharathi. A method of reducing the skew in reducer phase?□?block chain algorithm. In *Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on*, pages 1–4. IEEE, 2016.

[7]Junichi Kishigami, Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira, and Akihiko Akutsu. The blockchain-based digital content distribution system. In *Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on*, pages 187–190. IEEE, 2015.

[8]Wenbo Shi, Injoo Jang, and Hyeong Seon Yoo. A sealed-bid electronic marketplace bidding auction protocol by using ring signature. In *Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on*, pages 1005–1009. IEEE, 2009.

[9] Wee-Kheng Tan and Yung-Lun Chung. User payment choice behavior in e-auction transactions. In *e-Education, e-Business, e-Management, and e-Learning, 2010. IC4E'10. International Conference on*, pages 183–187. IEEE, 2010.

[10] Hu Xiong, Zhiguang Qin, Fengli Zhang, Yong Yang, and Yang Zhao. A sealed-bid electronic auction protocol based on ring signature. In *Communications, Circuits and Systems, 2007. ICCCAS 2007. International Conference on*, pages 480–483. IEEE, 2007.

[11] Shengbao Yao, Wan-An Cui, and Zhenqian Wang. A model in support of bid evaluation in multi-attribute e-auction for procurement. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*, pages 1–4. IEEE, 2008.

[12] Affan Yasin and Lin Liu. An online identity and smart contract management system. In *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual*, volume 2, pages 192–198. IEEE, 2016.

[13] Fangguo Zhang, Qiongfang Li, and Yumin Wang. A new secure electronic auction scheme. In *EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA*, pages 54–56. IEEE, 2000.

[14] Yan Zhu, Ruiqi Guo, Guohua Gan, and Wei-Tek Tsai. Interactive incontestable signature for transactions confirmation in bitcoin blockchain. In *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual*, volume 1, pages 443–448. IEEE, 2016.

[15] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE, 2015.

ISBN 978-1-5386-4342-6