Anonymous Verifiable Sealed Quotation Auction Based on Blockchain

Ke Wei[1,a*], Yulong Dang[1,b]

253111733@qq.com[a*], 2316772321@qq.com[b]

The State Key Laboratory of Tibetan Intelligent Information
Processing and Application
Qinghai Normal University, Xining China[1]

Abstract—With the development of blockchain technology, the existing online auction technology is developing from the trusted third party as auction intermediary to the disintermediation to the third party. Aiming at the problems existing in the existing sealed bid auction scheme based on blockchain, such as the leakage of bidders' privacy information, illegal acquisition or tampering of bidders' bids in sealed auction, etc. Based on blockchain as the bottom layer, an auction scheme with decentralization, bid privacy, anonymous verifiability, tamper-proof and collusion-proof is constructed. ASVChain uses encryption mechanism to encrypt each bidder's offer to ensure the privacy of the bid, and uses ring signature technology to sign the encrypted offer, providing safe and verifiable steps while ensuring that each bidder's personal information is not leaked, and preventing illegal tampering while resisting collusion. The security analysis shows the advantages of this scheme compared with the existing scheme. The experiment analyzes and tests the influence of the number of bidders on the bidding time, and the results show that the time consumption of the proposed auction scheme meets the daily auction demand.

Keywords-component; Keywords: blockchain; ring signature; homomorphic encryption; sealed auction; decentralizatio

1 INTRODUCTION

With the development of the Internet, a large number of traditional industries are changing towards digitalization. Auction is a very old industry, which can be traced back to ancient Babylon around 500 BC. With the intensification of the digital age, electronic auction has gradually replaced the traditional offline auction because it can break through the limitations of space, time and physics. Technavio's recent research shows that by 2026, the online auction market share of hard asset equipment is expected to increase to USD 2.12 billion[1], so electronic auction has greatly promoted the economic growth in the digital age.

Since American Pierre Omidyar founded eBay in 1995, electronic auction has developed for 26 years. Auction theory can prove that bidders and auctioneers can obtain the greatest benefits,

ICBBEM 2023, May 19-21, Hangzhou, People's Republic of China

DOI 10.4108/eai.19-5-2023.2334348

but a large number of actual cases show that Internet auctions have frequent auction cases due to the denial of bids by bidders, collusion among bidders, high intermediary fees charged by third-party platforms, and even collusion between third-party platforms and bidders. In the field of Internet auction, there are still many problems to be solved.

In 2008, the author of the pseudonym "Satoshi Nakamoto" published a paper called “Bitcoin: A Peer-to-Peer Electronic Cash System”[2]. In this paper, "Satoshi Nakamoto" first proposed the concept of Bitcoin. Bitcoin is a completely decentralized electronic cash system. Every time the participants who make transactions are independent and equal, the transactions between these participants do not depend on a trusted third party. With the deepening of researchers' research on Bitcoin, the core technology of Bitcoin has gradually been abstracted to form a new technology-blockchain. Blockchain has the characteristics of decentralization, high anonymity and traceability, which puts forward a brand-new solution to the problems faced by traditional electronic auctions.

The application of blockchain technology to electronic auctions mainly uses the decentralized characteristics of blockchain technology to reduce or even eliminate the control power of trusted third-party platforms for Internet electronic auctions. For auction parties who usually need to pay 8-20% commission, the transaction cost is greatly reduced. Without the existence of a third-party platform, there is no possibility of collusion between the platform and the auctioneer. At the same time, in the blockchain network, the security of the personal information of the auctioneer can be guaranteed through various signature technologies, and the auction is conducted through the blockchain, and each auctioneer is a node in the blockchain network, so as to ensure the fairness of the auction. In the auction stage, smart contracts provide an automated auction process. No matter what the auction logic is, it is very convenient and fast to define it with smart contracts and execute it automatically. Blockchain also provides a safe and traceable mechanism. Every step of each auction can generate a new block and link it behind the previous block. By virtue of the non-tampering of blockchain, when legal disputes arise between the two parties, it can provide credible evidence through blockchain. Therefore, combining blockchain technology with electronic auction can build a safe and credible auction environment for electronic auction. There are also some problems in online auction based on blockchain, such as it is difficult to resist collusion, malicious forgery of bids to destroy the auction and easy disclosure of personal privacy. Some existing work has provided some solutions to some extent. In order to better protect the auction based on blockchain, this paper combines homomorphic encryption technology and ring signature technology to construct an anonymous verifiable sealed bid auction model based on blockchain. The main contributions of this paper are as follows:

- Based on ring signature and homomorphic encryption algorithm, an anonymous verifiable auction model based on blockchain—ASVChain is constructed and implemented.
- ASVChain not only protects the privacy and safety of bidders on the blockchain auction network, but also prevents the bidder's tender disclosure from causing the auction fairness to be lacking.
- By comparing the existing schemes, ASVChian fills the shortcomings while retaining the advantages of most auction schemes. By comparing the schemes of SBRAC [19] and Li [20] through experiments, ASVChain has lower time consumption and better performance.

2 RELATED WORK

Electronic auction has produced a large number of research results in the past 26 years, such as double auction design of multi-unit [3]and sealed bidding auction based on fuzzy TOPSIS method[4], etc. The existing research on electronic auction mainly focuses on the application of auction mechanism in resource sharing, and Zhang et al. summarized and studied the resource sharing with the existing electronic auction[5]. With the popularization of blockchain technology, researchers have found that the combination of blockchain technology and auction theory can provide a traceable and credible auction environment for existing electronic auctions.

The research on sealed auction based on blockchain has been hot in recent years. Through the database retrieval analysis provided by Web of Science, the research on sealed auction based on blockchain has been increasing year by year since 2018. he article abstracts provided by the Web of Science in recent five years are co-presented by using VosViewer. The existing research on blockchain auction focuses on smart contracts, with smart contracts, trading markets and applications as three important pillars. Combined with bidding, consensus mechanism and p2p network, a research map based on blockchain sealed auction is constructed.

The research on sealed auction based on blockchain has made great progress since 2018. In 2018, Galal et al. put forward the solutions to prove zk-SNARKs by smart contract [6]and zero knowledge respectively[7], aiming at the trust problem of bidders and auction houses and how to ensure the public verifiability of auction results. The scheme of Galal et al. provides some good research ideas for sealed auction based on blockchain, but the research of Galal et al. cannot resist collusion. In the same year, CReam scheme was announced, and CReam realized an anti-collusion electronic auction system by designing smart contracts to resist collusion[8].

Pop et al. introduced Merlde proof algorithm into blockchain auction platform, and verified each bidder's bid based on Merkle proof algorithm to prevent false bid. Pop et al. implemented Merkle proof algorithm into English auction, Dutch auction and one-price sealed auction [9]. Amin et al. applied the concept of IOTA to the model based on the theory of sealed bid auction, and built an encrypted auction platform without miners [10]. Wang et al. combined blockchain with trusted execution environment and built Hybridchain to ensure the high performance and confidentiality of sealed auction [11]. Goichiro et al. applied the threshold encryption scheme to Bitcoin and tested its application in copyright protection, sealed auction and electronic lottery[12].

Sada and others have studied the energy sharing based on blockchain and sealed auction mechanism. Their main research is to use the auction mechanism based on blockchain to solve the energy transaction between electric vehicles and energy suppliers, and use the off-chain network to reduce the burden of blockchain [13]. Kwak et al. combined Vickrey auction theory, blockchain technology and Internet of Things to build the EggBlock platform to provide reliable and transparent transactions of solar energy[14].

Po-Chu Hsu et al. constructed an open and verifiable algorithm based on Vickrey auction theory, and implemented it on the Ethereum [15].Sarfaraz and others built an open bidding framework for blockchain, and used elliptic curve encryption and dynamic password accumulator encryption algorithms to strengthen the security of both auction parties[16].Abulkasim combines quantum computing and blockchain technology to design a sealed bid auction protocol[17].Sharma applies ring signature technology and zero-knowledge proof to sealed bidding auction. Ring signature provides anonymous and zero-knowledge proof of bidding to ensure the correctness of the insured[18].Li et al. put forward a sealed bid auction scheme based on blockchain, which uses Pedersen to promise to protect the bidder's bid price from being leaked, and uses zero-knowledge proof protocol to verify the correctness of the winning bid price[20].Chen et al. combined zero-knowledge proof with anonymous veto network to construct a blockchain sealed auction scheme with bid price privacy and public verifiability[19].

The existing research on sealed auction based on blockchain covers all the research on auction theory. However, most of the existing research on sealed auction based on blockchain can only guarantee one or more of openness and verifiability, anonymity, bid privacy, collusion resistance and decentralization. Therefore, it is imperative to construct an auction scheme with decentralization, anonymous bidding, bidding privacy, collusion resistance and openness and verifiability.

3 AUCTION SCHEME

This chapter is the process of realizing ASVChain model as ASVChain scheme. In the auction, each bidder’s bid is homomorphic encrypted to prevent malicious bidders from illegally stealing others’ bids. At the same time, combined with ring signature technology, the bidder’s key is hidden in the ring signature to ensure the anonymity and unforgeability of sealed bid auction, and at the same time, a verification algorithm is provided to ensure the verifiability of bids and complete the auction safely.

The whole process of ASVChain consists of auctioneers, blockchain networks, bidders and smart contracts. Blockchain network is formed in the form of blockchain and nodes. Auctioneers and bidders need to register before participating in the auction to determine their own identities. At the same time, as a node, they will join the blockchain network of the auction. For the joined client nodes, unique digital identifiers will be assigned to determine their identities, and public and private key pairs about individuals will be distributed. After the registration is completed, you can be an auctioneer or a bidder to release the auction task or participate in the auction.

When auctioning as a participant, the auctioneer initiates the auction, and the bidders encrypt their own quotations and identity digital identifiers as signature information for ring signature. The blockchain collects all the bidders’ ring signatures for verification, and analyzes the signature information of the verified signatures to obtain the bidders’ quotations and identity identifiers. After ranking the quotations, the highest quotation is selected as the winning bidder, and its signature is made public. Every bidder who participates in bidding can verify the signature of the winning bidder. Intelligent contract determines the winning bidder through digital token and promotes the transaction between the winning bidder and the bidder, and writes the transaction into the block, linking it after the previous block.

3.1 Anonymous verifiable auction algorithm

input：Bidder’s digital token Dt and quotation requiring signature m.

Output: Auction completed.

```
$AuctioneerSubmitsAuctionToBlockchain(Dt_A)$
**for** $i \in \{1,2,3,...,N\}$ **do**
    $(Pk_i, Sk_i) \leftarrow KeyGen1(1^k)$
// Obtain that public key and private key of the signature and form a public key set
**end for**
$(Pk^p, Sk^s) \leftarrow KeyGen2()$
**for** $i \in \{1,2,3,...,N\}$ **do**
    $BlockchainPostTobidder(Pk^p)$
// The bidder obtains the quotation encryption public key.
**end for**
**for** $i \in \{1,2,3,...,N\}$ **do**
    $(Mes_i, \delta_i) \leftarrow AnBid(m_i, Dt_i, Sk_i, Pk_v, Pk^p)$
    $BidderPostToBlockchain(Mes_i, \delta_i)$
**end for**
**for** $i \in \{1,2,3,...,N\}$ **do**
$(Sk^s, Mes_i, \delta_i) \leftarrow SmartconGetFromBlockchain()$
    **if** $OpBid(Mes_i, \delta_i)$ **then**
        $c_i \leftarrow Acq(Mes_i)$
    **end if**
**end for**
**for** $i \in \{1,2,3,...,N\}$ **then**
    **if** $c_i > HightestPrice$ **then**
        $HightestPrice \leftarrow c_i$
      $h \leftarrow i$
**end for**
```

```
$BiddersGetFromBlockchain(Mes_h, d_h)$
**for** $i \in \{1,2,3,...,n\}$ **then**
    **if** $OpBid(Mes_h, d_h)$ **then**
        **return success**
    **else return false**
$SmartconToBlockchain(Dt_h)$
$Account(Dt_h) \leftarrow Account(Dt_h) - HightestPrice$
$Accout(Dt_A) \leftarrow Accout(Dt_A) + HightestPrice$
*The auction is over*
```

4 EXPERIMENT AND ANALYSIS

The auction scheme studied is based on blockchain technology, and the ring signature technology is used to ensure the hiding of the bidder's public and private keys. If the individual key is signed into the ring signature, only the legality of the signature can be verified, but the individual key information can not be obtained. Homomorphic encryption algorithm is used to encrypt individual bid values and digital tokens to prevent unfair competition among bidders.

4.1 Security analysis

a)Correctness: The auctioneer chooses the highest price as the winning bidder in the commitment stage of the public winning bidder to ensure the correctness of the auction. In the selection of the highest bid, all bids are automatically sorted by smart contracts. External data cannot interfere with it.

b) Sealing: confidentiality requires that malicious bidders cannot obtain the real bids of other bidders. If a malicious opponent can destroy secrets, it means that it can get other people's bids in advance. Then, he can adjust the bid according to the obtained information, thus undermining the fairness among bidders. In this scheme, all bidders' bidding information will be encrypted by homomorphic encryption algorithm, and then signed as a ring signature message. Even if a malicious bidder obtains a bid quotation, it is only an encrypted quotation, and at least three encrypted quotations need to be decrypted.

c) Fairness: Using encryption algorithm to hide bidders' quotations makes all bidders in a fair auction environment. At the same time, ring signature ensures the fairness of personal privacy. Even if there is malicious conspiracy to bid at a low price in the network, as long as one of the bidders is just, then the auction is still valid.

d)Anonymity: For the auctioneer, all information is private in the blockchain network, even the personal key. The ring signature is made by a personal public key and a multi-person public key, and it is basically impossible to crack the ring signature.

e)Non-repudiation: the ring signature is verifiable, and the encrypted personal digital token and quotation are used as information to sign, and one information corresponds to one signature. Through verification, it can be determined whether it is a bidder's bid, which cannot be denied. Similarly, even if a malicious bidder attempts to forge someone's bid, once the bid is modified, the signature information will change, which will not pass the verification algorithm and will be discarded as an invalid bid.

f)Open verifiability: Not only the blockchain can verify the bid provided by this scheme, but also the unsuccessful users can verify the correctness of the winning bidder's signature through the verification algorithm to ensure that the winning price is available.

4.2 Experimental Analysis

Based on Hyperledger Fabric, an open source alliance chain, 8-core CPU, 16GB memory and Ubuntu16.04 operating system, this paper realizes the ASVChain model. By adjusting the number of nodes participating in the auction, the time consumption under the auction of 4, 5, 6, 7 and 8 people was tested respectively. And by comparing the time consumption of SBRAC[19] and Li[20].

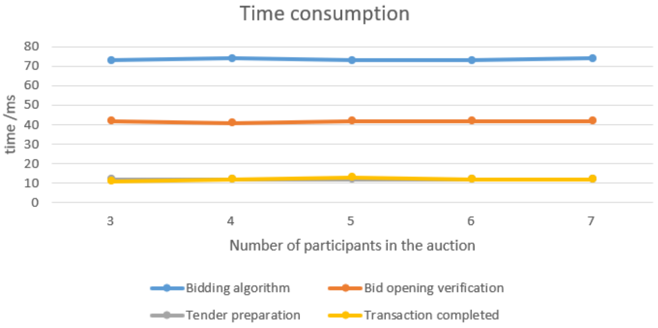

Fig 1. Time consumption

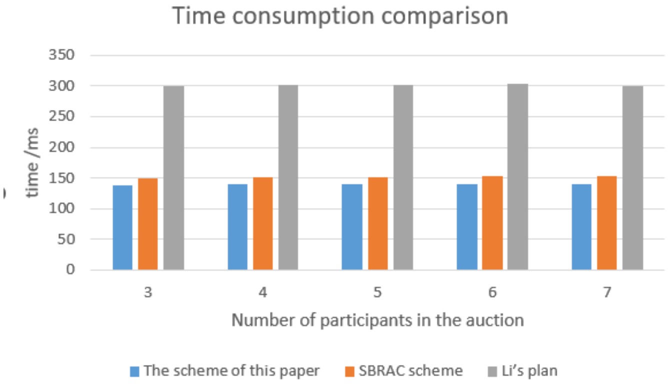

Fig 2. Time consumption comparison

Reference [6] proposed a verifiable blockchain auction model based on zero-knowledge proof, and provided a verifiable protocol. Compared with the method proposed in this paper, it lacks the protection of personal information and is difficult to resist collusion. Literature [17] uses quantum computing to provide difficult-to-solve security keys. Compared with the method proposed in this paper, it lacks public verification of bids and cannot resist collusion. Literature [10] uses an encryption algorithm with better encryption effect, which provides the bidder's identity hiding and identity verification for the auction based on blockchain. Compared with the method proposed in this paper, it can't resist collusion. Literature [19] gives a verifiable auction scheme with bid encryption, but it is weak in collusion resistance and privacy protection.

The study evaluates the performance by testing the time cost of each function under different numbers of bidders. As shown in Figure 1, with the increase of the number of bidders, the time consumption of the algorithm is relatively stable. If other bidders have no objection to the selection of the highest bid, it will take about 140ms to complete an auction. Therefore, the research scheme can meet the basic auction environment.

In order to ensure the advancement of this study, the time consumption of auction is compared with the recent domestic and foreign papers with similar types. SBRAC [19] is a relatively recent research, and its design idea is similar to that in this section. It uses zero-knowledge proof and anonymous veto network to achieve the requirements of anonymous anti-collusion, and achieves a good result. As shown in Figure 2, this paper compares the time consumption of SBAC [19], and this paper is slightly better than SBAC [19]. At the same time, literature [20] is compared, which is a relatively new paper on blockchain auction in China recently. By comparing the time consumption, the auction time consumption of the research scheme is almost half of that of literature [20], which has high efficiency.

5 Conclusions

This paper proposes an anonymous verifiable sealed bid auction scheme based on blockchain. This scheme combines ring signature with homomorphic encryption, which can ensure that the quotation will not be leaked while resisting collusion. As long as there is a just bidder in the bidding, collusion will not succeed. Ring signature provides anonymous and verifiable steps, which ensures personal privacy and provides public and verifiable steps. Every bidder participating in the auction can verify the bidding results while putting an end to forgery.

Smart contracts provide fixed and automated program execution to prevent auction fraud. However, although ASVChain guarantees the anonymity and privacy when bidding, it still needs a lot of manual review before the auction to see whether the auction items provided by the auctioneer are infringing, and whether it is possible to combine artificial intelligence technology to build an artificial intelligent blockchain auction platform, which needs to be considered in future work.

REFERENCES

[1] Technavio. Global hard asset equipment online auction market 2022– 2026.2022, https://www.technavio.com/report/hard-asset-equip -ment-online-auction-market-industry-analysis.

[2] Bitcoin: A Peer-to-Peer Electronic Cash System[J]. Social Science Electronic Publishing.

[3] Huang P , Scheller-Wolf A , Sycara K . Design of a Multi–Unit D- ouble Auction E–Market[J]. Computational Intelligence, 2010, 18(4).

[4] Singh R K , Benyoucef L . A fuzzy TOPSIS based approach for e-s- ourcing[J]. Engineering Applications of Artificial Intelligence, 2011(3):437-448.

[5] Yang Z , Lee C , Niyato D , et al. Auction Approaches for Resource Allocation in Wireless Systems: A Survey[J]. IEEE Communications Surveys & Tutorials, 2013, 15(3):1020-1041.

[6] Galal H S, Youssef A M. Verifiable sealed-bid auction on the ethereum blockchain[C]// International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2018: 265-278.

[7] Galal H S, Youssef A M. Succinctly verifiable sealed-bid auction smart contract[M]//Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, Cham, 2018: 3-19.

[8] Wu S , Chen Y , Wang Q , et al. CReam: A Smart Contract Enabled Collusion-Resistant e-Auction[J]. IEEE Transactions on Information Forensics and Security, 2018:1687-1701.

[9] Pop C , Prata M , Antal M , et al. An Ethereum-based implementa- tion of English, Dutch and First-price sealed-bid auctions[C]// 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP). IEEE, 2020.

[10] Amin H M S , Sufiyan Z , Rafi N , et al. Secured IOTA Enabled Crypto-Platform with Discretionary Mining Capabilities and Miner Nomination based on First-Price Sealed Bid Auction Theory[C]// 2020 IEEE Region 10 Symposium (TENSYMP). IEEE, 2020.

[11] Y. Wang, J. Li, S. Zhao and F. Yu, "Hybridchain: A Novel Archi- tecture for Confidentiality-Preserving and Performant Permissioned Blockchain Using Trusted Execution Environment," in IEEE Access, vol. 8, pp. 190652-190662, 2020,
doi: 10.1109/ACCESS.2020.3031889.

[12] Goichiro, HANAOKA, Yusuke, et al. A Setup-Free Threshold Encryption Scheme for the Bitcoin Protocol and Its Applications[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2020, E103.A(1):150-164.

[13] Al-Sada B , Lasla N , Abdallah M M . Secure Scalable Blockchain for Sealed-Bid Auction in Energy Trading[C]// IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2021.

[14] Kwak, Subin, Joohyung Lee, Jangkyum Kim, and Hyeontaek Oh. 2022. "EggBlock: Design and Implementation of Solar Energy Generation and Trading Platform in Edge-Based IoT Systems with Blockchain" Sensors22, no. 6:2410.https://doi.org/10.3390/s22062410

[15] Hsu P C, Miyaji A. Bidder Scalable $\mathrm {M}+ 1\text {st} $-Price Auction with Public Verifiability[C]//2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2021: 34-42.

[16] Sarfaraz A , Chakrabortty R K , Essam D L . A Tree Structure-bas- ed Improved Blockchain Framework for a Secure Online Bidding System - ScienceDirect[J]. Computers & Security, 2020.

[17] Abulkasim H , Mashatan A , Ghose S . Quantum-based Privacy-Pre- serving Sealed-bid Auction on the Blockchain[J]. Optik - International Journal for Light and Electron Optics, 2021:167039.

[18] Sharma G, Verstraeten D, Saraswat V, et al. Anonymous Sealed-Bid Auction on Ethereum[J]. Electronics, 2021, 10(19): 2340.

[19] Chen B, Li X, Xiang T, et al. SBRAC: Blockchain-based sealed-bid auction with bidding price privacy and public verifiability[J]. Journal of Information Security and Applications, 2022, 65: 103082.

[20] LI Bei, ZHANG Wenyin, WANG Jiuru, ZHAO Wei, WANG Haifeng. Sealed-bid auction scheme based on blockchain[J]. Journal of Computer Applications, 2021, 41(4): 999-1004.