Secure E-Tender Allocation Using Blockchain

Vipul Kumar[1, a)], Vishwaas Saxena[2, b)], Shivangi Pandey[3, c)] and Neha Yadav[4, d)]

[1,2,3,4] *Department of Computer Science and Engineering, KIET Group of Institutions, Ghaziabad, Uttar Pradesh, India*

[a)] Corresponding author: vipulmy10@gmail.com
[b)] vishwaas7saxena@gmail.com
[c)] shivangipandey.r@gmail.com
[d)] nehayadav1508@gmail.com

Abstract. Organizations in the public sector's permissionless blockchain, including those in the government, are working to discover new means to stay in operation. Along with technological progress, cost reductions, wise governance, and work efficiency. Blockchain technology is one such innovation that has recently attracted the attention of governments all around the world. The blockchain's increased security, enhanced traceability, and lowest-cost infrastructure allow it to penetrate numerous industries. Governments frequently issue tenders to a small number of outside companies for a variety of projects. Many competitors attempt to overhear out the tender values of their rivals to win the contract. Furthermore, dishonest government representatives seek a sizable bribe in exchange for passing the offer to a third party. In this work, we present a blockchain-based architecture for public procurements that are both secure and efficient.

Keywords: Blockchain, Ethereum, Smart Contracts, Decentralized system, Tender Allocation

INTRODUCTION

Nearly all industries and regions of the world have seen a significant increase in the usage and acceptance of blockchain technology. To improve the level of safety, confidentiality, transparency, and work efficiency, government tender processes can make use of up-and-coming blockchain technology [16]. Blockchain technology can make it possible for all parties interested in a given offer to be a part of the same network and to track the workflow in real time. Governments in countries like Georgia, the UK, the UAE, Australia, China, Japan, and Russia are integrating blockchain technology into their daily operations at a rapid rate nowadays [4][7]. In recent years, the governments of several developing nations, including India, are coming up with initiatives and regulations for the adoption of blockchain technology.

In practically all industries and regions of the world, the usage of blockchain technology has grown quickly. To increase the level of secure allocations, privacy, openness, and productivity throughout the government tender process, blockchain technology is a very promising alternative [11]. Blockchain technology enables all parties engaged in a tender to join a particular network and helps in real-time transaction monitoring of the network [1].

In other terms, blockchain is a digital ledger for transactions or contracts that need to be recorded. It is a secured, distributed database that stores data [16][10]. In practically all industries and regions of the world, the usage of blockchain technology has increased more quickly. Online reservation systems, modes of digital acquisition, and the submission of tax returns, and other things, are only a few examples of the numerous initiatives undertaken to apply innovations to develop paperless and quick government procedures. Despite these systems being well-designed and implemented, all of them are based on the idea that a host could fail because attackers could easily hack or prevent it from functioning using attacks like DOS attacks, and Man in the Middle attack, among others [17]. In most nations, complex regulatory requirements result in faulty workflows that are plagued with corruption, inefficiency, and human neglect. Several governance processes, including government tenders, involve data leakage, dishonesty, and bribery [5]. By tackling these problems, we hope to create a transparent and more safe fog computing infrastructure for the

distribution of contracts that besides doing away with the need and tendency for in-person oversight or intervention; makes it simple for the administration to monitor and revise its rules and policies over time. We suggest a formation to use blockchain technology to build a dispersed system to perform and look over government and its tendering processes easily, transparently, and immutably to address this problem [11].

BACKGROUND

Blockchain architecture is a shared database or public ledger of records or transactions used by many parties in a network. A blockchain network can be joined by a participant freely based on whether it is Permission-less (Public) or Permissioned (Private) [11]. Any user of a permissionless blockchain network, such as Bitcoin, is given a special address through which they can communicate with the network, enabling anyone to take part in the transaction validating process [1][10]. A closed environment known as a permissioned blockchain prohibits users from freely joining the network matrix, viewing the recorded ledger, or issuing exchanges [14]. The fact that a Permissionless Blockchain requires a lot of computational power to reach consensus and that the transaction history is publicly available is one of the main disadvantages that prevent the majority of businesses from utilizing it [13]. The participation of the general public is restricted by the permissioned blockchain, which places restrictions on the parties who can transact on the blockchain. As a result, we employ consortium blockchain, which takes advantage of both networks' strengths. While the transactions are only validated by the authorities and co-authors, common constructors or construction firms are permitted to join the network by adding their legitimate IDs [10]. Thus, a consortium blockchain offers an additional layer of privacy while nevertheless having all the key benefits of a permissionless network. Ethereum is one such platform that enables the development of distributed applications [10][17]. It is a cross-industry open-source collaborative project designed to improve blockchain technologies [3]. It enables the establishment of specific Confidential Channels that can maintain a distinct ledger that is only accessible to those who participate in that channel. Government offices can be divided into multiple departments, each of which has its own set of authorities that can view and verify transactions only related to that department [13].

RELATED WORK

There are several studies and examples of projects that have been made using blockchain technology for tender allocation. One notable project is the "Smart Tenders" platform developed by the European Union's Horizon 2020 research program. This uses blockchain technology to automate the evaluation of bids. This platform also allows users to build a reputation over time, which is used as an assessment parameter while providing contracts. Another example is the "Blockchain-based Public Procurement Platform" which is developed by the government of the Republic of Korea. This platform aims to increase transparency and reduce the risk of fraud in the public procurement process [16]. The platform uses blockchain technology to record all activities and allows all participants to access the same information. The "Blockchain-based e-Procurement System" which is developed by the government of Andhra Pradesh, India is also a recent example of the same. The system aims to automate the allocation process using blockchain technology to ensure the transparency and security of the process. The system also allows for the tracking of goods and services. In addition to these specific projects, there have also been several academic studies that have looked at the use of blockchain in tender allocation.

Overall, related work on blockchain-based tender allocation projects has shown that the technology has the potential to bring transparency, immutability, and security to the tendering process, along with automation and reduction in human errors.

PROPOSED WORK

Government lenders and builders first join the blockchain architecture to build a safe fog computing infrastructure. All relevant constructors are informed about the tender information by the government lender. The suggested concept is a decentralized and consortium architecture that blends the permissioned blockchain's security and privacy with the permissionless blockchain's openness and transparency. The concept aims to manage the government tender process securely and effectively. Government authorities, outside parties like construction corporations or individual contractors, and banks make up the system's core three sorts of entities. Based on identity identification, we can use Ethereum to restrict the network nodes' access to data [2][3]. The files are only accessible to the nodes that are authorized to examine or validate the specific data [13].

This system extensively uses smart contracts in its functioning to deploy the tender and the rest of the functioning which extends to score formulation and assignment of tenders to the winning party. Smart Contracts are contracts that may be enforced by the law and are written using standardized code and operational specifications [10][14]. Until and unless all the nodes of the network verify and flag the transaction as legitimate it cannot be added to the block. The final exchange history and the blockchain will both contain the transaction details when they have been confirmed, together with a timestamp and the parties' public keys [11]. A collection of key-value pairs are created as a result of the execution of smart contracts and are recorded and maintained on the ledger and preserved on the blockchain [7]. The implementation of the project is divided into these categories:

Creation of Tenders

Tender is created by the government for interested parties to bid and to be allotted to the potential party who is the most suitable according to the proposed parameters. Each tender has a unique name and id (tender key) and a description containing the nature of the tender and its requirements. The tender key keeps the record of the number of tenders created so far. Tenders have certain parameters that set the characteristics of the tender. Every tender has a fixed date stamp until which the interested parties can bid and accordingly, the bidding hash can be created.

Bid Parameters

These parameters are the set of characteristics or requirements that are specified for a tender, which is a formal invitation to submit a proposal for a project or supply of goods or services.

Time

The time parameter refers to the duration of the tender process, which is typically divided into two periods - the time between the opening and closing of the tender, during which parties can submit their bids, and the time for evaluating the bids and selecting a winner. The time parameter may also include specific deadlines for submitting bids, as well as any deadlines for clarifying or modifying the bid.

Price

The price parameter specifies the maximum or minimum price that can be offered in a bid. This can be a fixed price or a range of prices, and it may be based on a variety of factors such as the cost of materials, labor, and overhead. The price parameter may also specify any discounts or rebates that can be offered as part of the bid.

Environment

The environment parameter refers to the physical, social, or economic conditions in which the project or goods will be delivered. This could include factors such as the location of the project, the type of industry or market, and any relevant regulations or standards that must be met. The environment parameter may also specify any specific challenges or constraints that the bidder must consider when preparing their proposal.

Also, if any unauthorized organization tries to create a tender by invoking create tender function, then it will receive an error representing transaction failure. The below image shows the failed transaction.

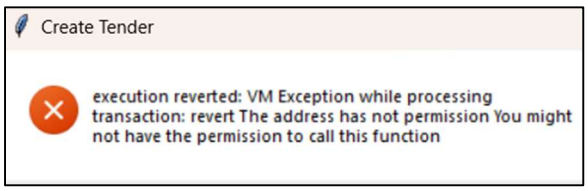

FIGURE 1. No permission to Create Tender

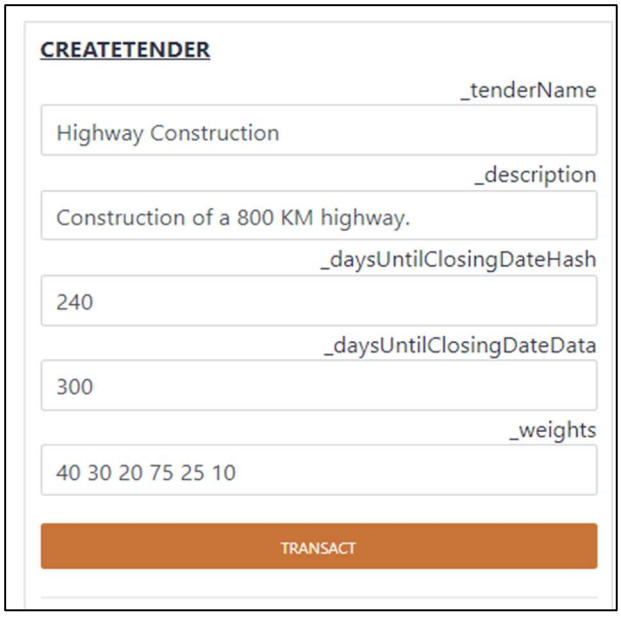

FIGURE 2. Create Tender

```
[6:43:44 PM]: Send data to method 'CreateTender'
with ["Highway Construction","Construction of a
800 KM highway.","240","300","40 30 20 75 25 10"]
from 0x5036Eb04d8cB1Ea96C1A87B0AEc00245787F154d at
contract address
0x4F5e74C63199C5FD5452fbe07c762790F30bd7B7
[6:43:45 PM]: TRANSACTIONHASH :
[6:43:45 PM]:
"0x955670355e26facd9b93ceafacae297bb71546727811159c
d3e66e6076856df7"
[6:43:45 PM]: BLOCKHASH :
[6:43:45 PM]:
"0xe7d28b901533c8863a4cb9269a06ab3e0fb4e70eb02ed51b
113003b97890adca"
[6:43:45 PM]: FROM :
[6:43:45 PM]:
"0x5036eb04d8cb1ea96c1a87b0aec00245787f154d"
[6:43:45 PM]: TO :
[6:43:45 PM]:
"0x4f5e74c63199c5fd5452fbe07c762790f30bd7b7"
[6:43:45 PM]: GASUSED :
[6:43:45 PM]: 439338
[6:43:45 PM]: CUMULATIVEGASUSED :
[6:43:45 PM]: 439338
```

FIGURE 3. Create Tender Output

Place Bid

The function placeBid is used to place a bid for a tender identified by the tenderKey argument. It takes in three arguments: tenderKey, firmAddress, and hashOffer.The bid is placed by a firm identified by the firmAddress argument, and the hashOffer argument provides a hash of the offer made by the firm. The function begins by retrieving the tender identified by the tenderKey argument from the tenders mapping and storing it in a variable named tender. Next, the function sets the AlreadyBid field of the tender to true for the firm identified by the firmAddress argument. This indicates that the firm has already placed a bid for this tender and cannot participate in the tender anymore [1][8].

Finally, the function creates a new BidOffer object for the tender and assigns it to the bids field of the tender for the firm identified by the firmAddress argument. The BidOffer object is initialized with the following values:
Firm Address: the firm placing the bid
Hash Offer: the hash value of the offer.

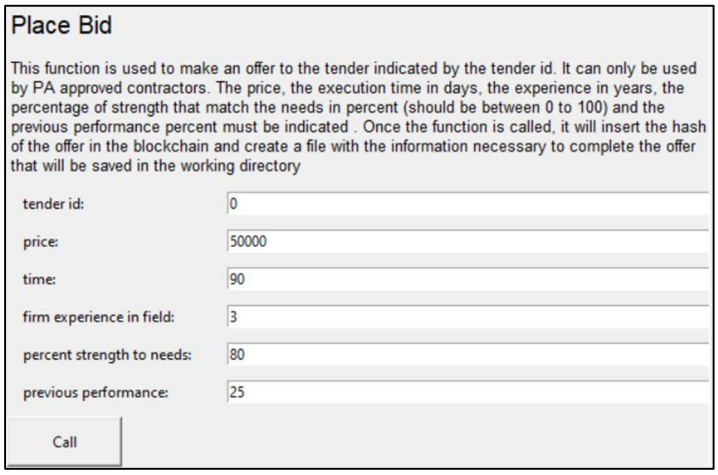

FIGURE 4. Place Bid

Concluding Bid

The function for concluding whether a bid is valid or not is named concludeBid and it takes in four arguments: tenderKey, firmAddress, bidValues, and separator. The function is used to conclude a bid for a tender identified by the tenderKey argument. The bid is placed by a firm identified by the firmAddress argument. The values of the bid are provided in the bidValues argument, and the separator argument indicates the separator that arises between these values. The function begins by retrieving the tender identified by the tenderKey argument from the tenders mapping and storing it in a local variable named tender.

Next, the function sets the values field of the bid placed by the firm identified by the firmAddress argument to the bidValues argument. The separator field of the bid is also set to the separator argument. Finally, the valid field of the bid is set to true to indicate that the bid is now considered valid.

Score Formulation Parameters

Previously, we were using three main parameters - **time, price,** and **the environment** - to determine the result of a bid. Now, we are dividing the environment parameter into subcategories to calculate the score for the environment variable. The environment parameter is used to evaluate the impact that a bidder's work will have on the environment. Dividing it into subcategories allows for a more detailed evaluation of this impact. Also, it becomes easier to accurately assess the environmental impact of a bidder's work. These subcategories include the **firm's experience** and the **percentage of matching** between the contract requirements and the company's strengths. In addition to these three parameters, a fourth parameter - the **firm's deliverance rate** - is being introduced. These four parameters will be used to formulate the original score of the bidder, which will be used to calculate the result.

The subcategories of the environment parameter will have fixed weights that will be used to calculate its score. Once the environment score has been determined, variable weights will be applied according to the needs of the tender to calculate the overall score, which will be used to determine the winner. Once the scores for each of the subcategories have been calculated, they can be combined to formulate the overall score for the environment parameter. This score can then be used along with the scores for the time and price parameters to determine the final result of the bid.

Assign the Winner

After the scores are formulated for each of the bidders, all of these scores are saved along with the data of the bidder. To assign the final winner of the bidding process, an iterator iterates through all the participants of the bidding process and checks for the maximum formulated score present in the data structure, as the maximum score is known after the completion of the iteration, and the winner is assigned.

RESULTS AND ANALYSIS

The results of the simulation showed that the blockchain-based system was able to provide a tamper-proof record of the tender process, increasing transparency and reducing the potential for fraud. Additionally, the system was found to improve efficiency by automating the process through the use of smart contracts. The smart contracts were able to ensure that all the terms of the contract were met and that the process was completed quickly.

With the help of blockchain, we have come up with a transparent and safe e-tender allocation system for efficient tender allocation while maintaining the security of contracts and the privacy of the bidders. In our implementation, we have used a Python interface based on tkinter to communicate with the contracts. Using which we can easily view the details of the tender, analyze and view the bidding details of the winner and the participants once the winner has been declared. Using this interface all the other participants can view the details of all other bidders and gain experience as to bring about changes in their future bids. If in any case any participant tries to access the details of other bids, an error will be displayed, and the data will not be accessible before the final results of the tender are out. This provides complete secrecy and prevents any breach of data leading to the cause of unfair decisions.

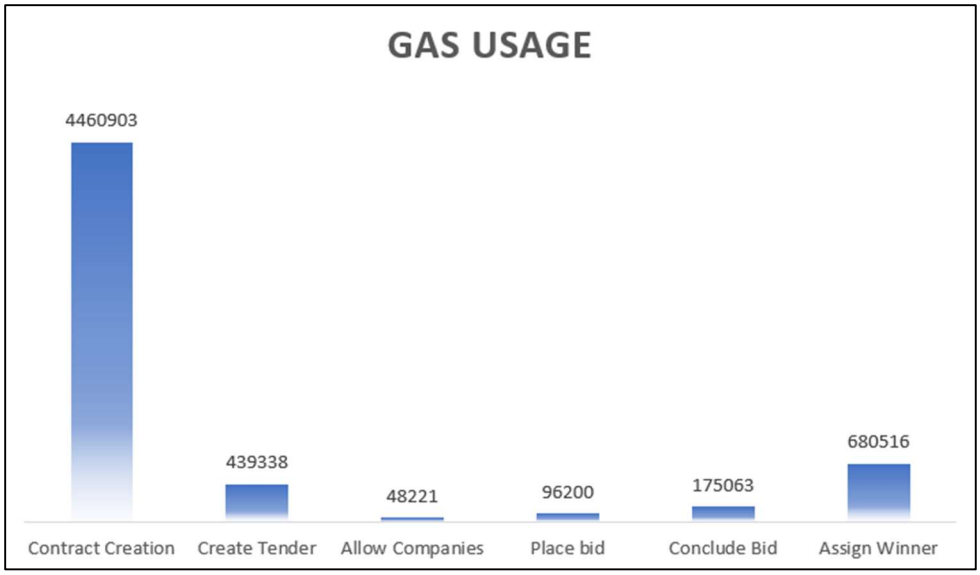

FIGURE 5. Gas Usage Bar Graph

Gas Usage Analysis

It gives an estimate of the complexity of various functions in the contract. It is related to the complexity of blockchain transactions. The blockchain transaction gets reverted if the transaction uses more gas than the specified gas limit. The higher the gas usage of a function, the higher will be its transaction fee.

The figure above is a bar graph depicting the gas usage of different transactions of the blockchain. The contract creation has the highest gas usage when compared with others which accounts for the complexity of the function. The product of gas usage and gas value gives us the transaction fee of the function. Generally, the gas value is taken to be 1 GWEI.

CONCLUSION

This paper is explained in the context to impress blockchain technology as a means to create a tender allocation system. We have discussed significant opportunities that the technology offers while focusing on transparency. The algorithms are traceable and secure ensuring the bidding process is genuine. Ethereum has been used as a means to connect edge-to-edge frameworks [10]. Mechanisms are designed in a way to yield maximum profits to the government and the lenders. In comparison to the other models, the suggested one yields better results and is interactive. We are upon aim to develop and cater to broader needs.

FUTURE SCOPE

Our work regarding this technology is to incorporate all the literary sources and surveys on the importance and conjecture of blockchain technology along with web security. We aim to project meaningful data to the users along with upvoted factors. We are trying to unveil the current trends of this technology and further ignite future research. The trends in this area of blockchain have been accelerating for the past five years. We are trying to answer numerous questions with our approach:

What changes did our model bring in the course of this project?
Why pursuing our model is better?
Why are the challenges in the future aspect of Blockchain in this domain?

REFERENCES

1. V. Hassija, V. Chamola, D. N. Gopala Krishna, N. Kumar and M. Guizani, "A Blockchain and Edge-Computing-Based Secure Framework for Government Tender Allocation," IEEE Internet of Things Journal **8**, 2409-2418 (2021).
2. A. Ambegaonker, U. Gautam and R. K. Rambola, "Efficient approach for Tendering by introducing Blockchain to maintain Security and Reliability," in *2018 4th International Conference on Computing Communication and Automation* (ICCCA) (Greater Noida, India, 2018), pp. 1-4.
3. Charles E Darwin1, Avinash Kothandan2, Athmanathan M3, Shanthi S 4, "Tender Allocation using Blockchain Technology" in 2022 International Journal of Creative Research Thoughts (IJCRT) **10**, (2022).
4. Mihir Bellare and Phillip Rogaway, *Introduction to Modern Cryptography,* (Davis, University of California, 2005), p. 10.
5. Betts, Martin & Black, Peter & Christensen, Sharon & Dawson, Ed & Du, Rong & Duncan, William & Foo, Ernest & Nieto, Juan, "Towards secure and legal E-tendering," Journal of Information Technology in Construction **11**, 89-102 (2006).
6. Ravina More, Pratiksha Kadam, Tejal Phadtare, Ketaki Bhagat, Prof. C.S. Wagh, "Secure Framework for Government Tender Allocation using Blockchain", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) **2**, (2022).
7. Dr. W. Gracy Theresa, Kishore.G, Kishan Kumar V, Mohamed Shafiq J, "A Blockchain and Edge Computing-based Secure Framework for Government Tender Allocation," International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET) **10**, (2021).
8. D. Mali, D. Mogaveera, P. Kitawat and M. Jawwad, "Blockchain-based e-Tendering System," in *2020 4th International Conference on Intelligent Computing and Control Systems* (ICICCS) (Madurai, India, 2020), pp. 357-362.
9. Li Li, Jiayong Liua, Peng Jia SecTEP "Enabling secure tender evaluation with sealed prices and quality evaluation in procurement bidding systems over the blockchain", Computers & Security **103**, 102188 (2021).
10. Svein Ølnes and Arild Jansen "Blockchain Technology as s Support Infrastructure in e-Government," in *International Conference on Electronic Government*, (Springer, 2017), pp. 215-227.
11. Y. Zhang, S. Deng, Y. Zhang and J. Kong, "Research on Government Information Sharing Model Using Blockchain Technology," in *2019 10th International Conference on Information Technology in Medicine and Education* (ITME, 2019) (Qingdao, China, 2019), pp. 726-729.
12. S. Rama, S. V. Flowerday, and D. Boucher, "Information Confidentiality and the Chinese Wall Model in Government Tender Fraud," in *2012 Information Security for South Africa* (IEEE, 2012), pp. 1-8.
13. H. Hou, "The Application of Blockchain Technology in E-government in China", in *2017 26th International Conference on Computer Communication and Networks* (ICCCN) (IEEE, 2017), pp. 1-4.
14. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (BigData Congress)* (Honolulu, HI, USA, 2017), pp. 557-564.
15. Min Xu, Xingtong Chen and Gang Kou "A systematic review of blockchain", Financial Innovation 5, 27 (2019).
16. D. Xu and Q. Yang, "The Systems Approach and Design Path of Electronic Bidding Systems Based on Blockchain Technology," Electronics **11**, 3501, (2022).
17. Thilak K, Prof. Priya N "Smart Tender/Contract Management System Using Blockchain", International Research Journal of Modernization in Engineering Technology and Science **4**, (2022).