IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104139 |

Web Based Tender Management System using Blockchain

Rohit Bikkad, Ganesh Choudhary, Swaraj Halikar, Arnav Gajbhiye, Prof. Pragati Deole

UG Student, Department of C.S., Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

UG Student, Department of C.S., Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

UG Student, Department of C.S., Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

UG Student, Department of C.S., Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Asst. Professor, Department of C.S., Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

ABSTRACT: The tendering procedure is typically used by businesses and governments to obtain goods or services from producers or service providers. The most popular mode of procurement, e-tendering, has a number of security problems. As it primarily emphasizes information decentralization and is protected by encryption combined with an unquestionable block-based design for transaction management, blockchain technology can be used to address these security problems. This study examines the use of smart contracts, which are built on the Ethereum blockchain, to create a distributed e-tendering system.

KEYWORDS: Blockchain, Fair and Open Tendering Scheme, smart contract, Ethereum, e-tender.

I. INTRODUCTION

The "Web Based Tender Management System" is a concept for online tender publishing. Tender information is included in it, along with information on the products, requirements, and terms. Until the tender's closing date, published tenders will be available to site visitors.

Numerous enormous businesses manage sizable/large projects for the government and other private businesses. There would be thousands of workers engaged in all such projects. Such a business needs to buy from multiple vendors for diverse needs. By placing advertisements in reputable media, the staff would announce global tenders. Newspaper advertising is expensive, and newspaper searches take a lot of time. Additionally, it takes a long time to receive bids, finalise tenders, and bridge the communication gap between buyers and suppliers (the only channels are phone or mail). Therefore, we do the entire tendering process online, which is quick and effective. Testing Goal: To confirm that the system will operate in accordance with the requirements. The information is not shared with all stakeholders under the current "fair and open" E-Tendering methods (Right to Information). When a company is chosen as the winner of a contract, other companies that submitted bids on the same tender are not informed of why their bid was rejected and why a specific company was chosen as the winner. This is because the information is disclosed "when they please." Although it is a laborious process, a firm can seek this information. Although auditing these records is a possibility, it takes time to evaluate the materials. Security is a serious problem for these portals, which contributes to fraud and the manipulation of data held in a centralised database in addition to the lack of transparency.

These security issues can be solved with blockchain technology, which strongly emphasises information decentralisation, is protected by encryption, and has an undisputed block-based design for transaction administration.As a result, blockchain technology and smart contracts can be used to establish a transparent, decentralised, and secure tendering framework that enables bidders to track portal operations and all actions taken by the tender site.

Traditional technology and design patterns cannot be employed in applications like tender portals because they jeopardise the criteria for security and transparency, which are of the utmost significance. As was previously mentioned, using a centralised tender platform for contract creation and bidding will not enough to meet all of the security requirements for a tendering framework. Only fair, open, decentralised technology, like blockchain and smart contracts, can address the security needs and transparency requirements for this kind of application.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104139 |

II. RELATED WORK

Kenneth Culp Davis - Government records must be made available to "any individual," unless one of the nine exemptions or other requirements are "clearly mentioned" in the Information Act, which went into force on July 4, 1967. District courts have the authority to compel an agency to turn over records. The Act is challenging to understand, and it was poorly written in several places.

AjeenkkyaAmbegaonker- The system that is previously proposed acts as an incentive to systematise the tendering processes of tendering organisations with the aid of blockchain's tools and technologies, enabling them to capitalise on a number of advantages of e-Tendering, including efficiency in terms of computation and cost of procurement, shortened tendering cycles, full transparency throughout the entire process, avoidance of human discretion/interference that will result in fewer mistakes, and availability. Greater security would be provided by blockchain implementation as opposed to traditional database-based internet applications. As a result of this system's ability to allow global tendering organisations to submit their bids on the blockchain, bidders can choose from a variety of projects without any issues, and access is also made possible.

Om Pal, Surendra Singh- We covered a number of aspects of blockchain technology in this essay, including its data structure, smart contracts, open source blockchain platforms, consensus mechanism, network transactions, etc. We talked about the different fields in which this technology can be used, as well as the way that blockchain technology is implemented in e-tendering.

Zibin Zheng- The four main qualities of blockchain—decentralization, persistency, anonymity, and auditability—have demonstrated their potential to revolutionise traditional industries. We give a thorough explanation of blockchain technology in this essay. We begin by providing an introduction to blockchain technologies, including an explanation of its architecture and its main features. The common consensus algorithms utilised in blockchain are then covered.

Marc Pilkington- The fundamental ideas underlying blockchain technology are explained in this chapter, along with some of its cutting-edge uses. We start by outlining the fundamental ideas behind the blockchain. In the second section, we analyse a definition proposed by VitalikButerin, outline the shift toward hybrid solutions, and list the key characteristics of decentralised public ledger platforms. Thirdly, we demonstrate the fundamental importance of the blockchain while exposing the possible dangers and shortcomings of open-source distributed ledgers, which are responsible for the shift to hybrid solutions.

WENBO WANG1 - A thorough analysis of the most recent advancements in blockchain technology is offered in this paper, with a focus on the designing processes and related research for permissionless consensus protocols. We started our in-depth examination into the architecture of consensus protocols and their influence on the newly developing applications of blockchain networks from the survey's concise review of the implementation stacks for blockchain networks.

Christian Cachin- The process of evaluating and establishing trust in a consensus protocol's robustness when it is exposed to flaws and hostile nodes is covered in this study. We urge designers of numerous practical systems to adhere to accepted practises in cryptography and computer security by relying on thorough models, rigorous justifications, and open reviews. In addition, we examine the fault models and attack resistance of certain well-known permissioned blockchain platforms' consensus protocols.

Karthikeyan Bhargavan- According to our preliminary research utilising F? to validate smart contracts, the type and eect system of F? is capable of capturing and demonstrating desirable qualities for contract programmers. Our method, which is based on shallow embeddings and typechecking inside of an established veri cation framework, is practical for investigating the formal veri cation of contracts written in Solidity and EVM bytecode. However, some languages' specific static tools might be simpler to use. (For instance, we lack tools that can plainly describe F? typechecking failures in source-code.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104139 |

III. PROPOSED SYSTEM

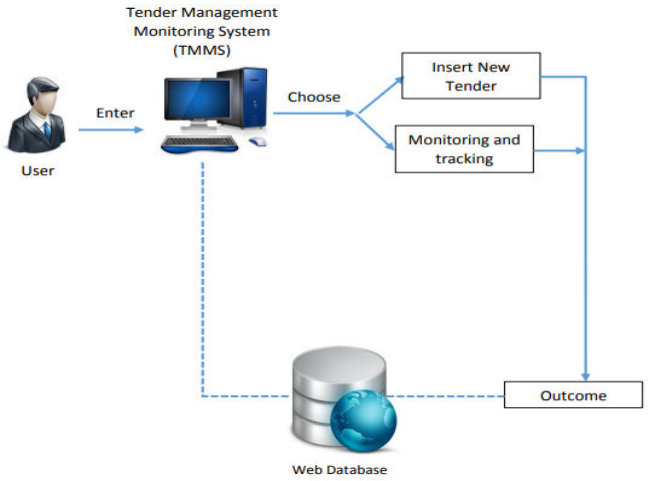

Fig.1. System Architecture

This project's development would involve various facets. The methods and procedures used in the project procurement management department's tender cycle are included in the first scope. It is best to initially acquire knowledge of this subject before moving further with system development. Once sufficient data is gathered, the system development process can begin. It is thought that interviewing people and adopting a self-experience technique are the best ways to learn this information. The development of the system itself is the second scope that is included throughout the process. Before choosing a platform for the creation of a database system, references must be made. The first objective should be to observe and differentiate various database developer platforms while considering the characteristics that the system offers. The knowledge gained through this procedure should be kept on hand for future reference. Another new area of study is included, with a focus on system development. Learning focuses on the syntax of the programming language used in system development. Programming language and coding errors would teach the developer something new. The development of the system would be improved by individual skill improvement.

IV. PROPOSED ALGORITHM

A. ***AES(Algorithm for Encryption)****:*

Advanced encryption standard, or AES.The algorithm is symmetrical. It used to cypher text from plain text.Due to DES's shortcomings, this algorithm was necessary. Des's 56-bit key is no longer secure against attacks based on thorough key searches, and the 64-bit block is likewise seen as vulnerable.The 128-bit block and 128-bit keys of AES were to be employed.Rijendeal was founder. It is being used in this drop to encrypt the data owner file

Input:

128_bit /192 bit/256 bit input (0, 1)

Secret key (128_bit) +plain text (128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256 bit input

X or state block (i/p)

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104139 |

Final round:10,12,14

Each round consists: sub byte, shift byte, mix columns, add round key.

Output :

cipher text(128 bit)

B. ***MD5 (Message-Digest Algorithm)***:

A common cryptographic hash function is the MD5 message-digest algorithm, which generates a 128-bit (16-byte) hash value that is generally written in text form as a 32-digit hexadecimal number. In addition to being frequently used to check the integrity of data, MD5 has been employed in a wide range of cryptographic applications.

Step 1: A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.
Step 2: The output of a message digest is regarded as the input data's digital signature.
Step 3: A message digest technique called MD5 generates data in 128 bits.
Step 4: It makes use of trigonometric Sine function-derived constants.
Step 5:It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.
Step 6:Most contemporary programming languages include with built-in functions for the MD5 algorithm.

V. RESULTS

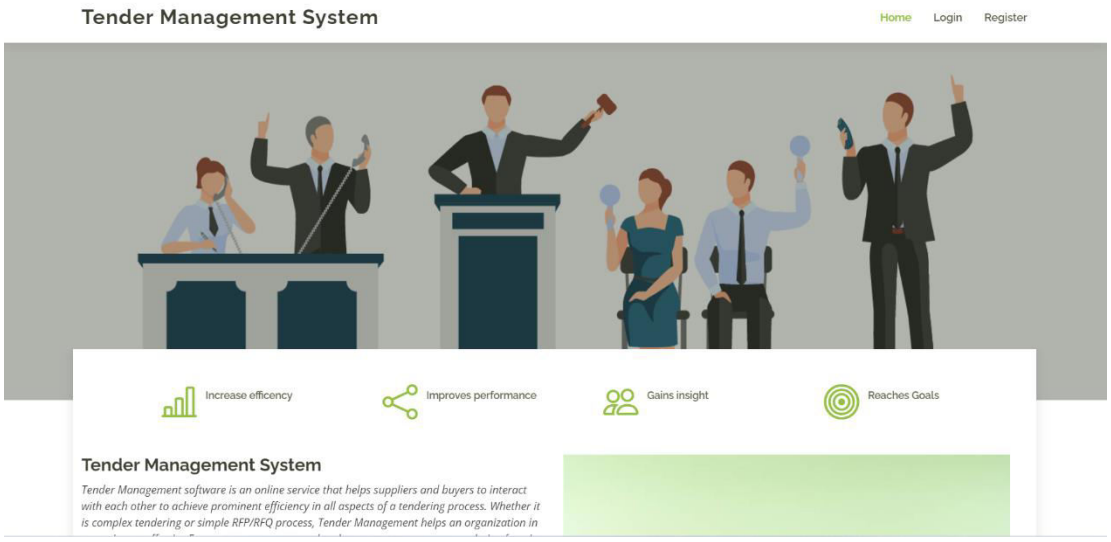

Fig.2. Home Page

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104139 |

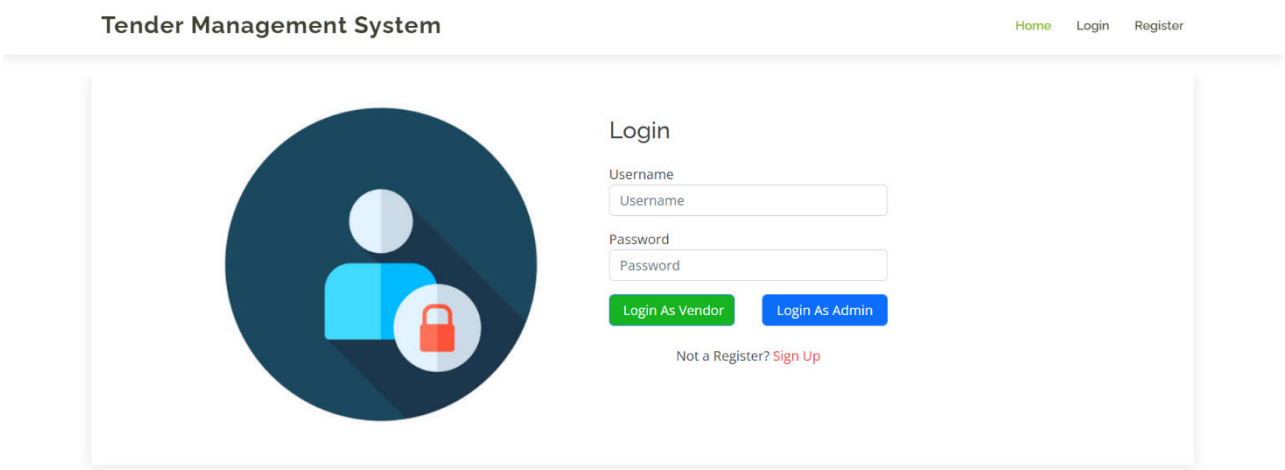

Fig.3.Login Page

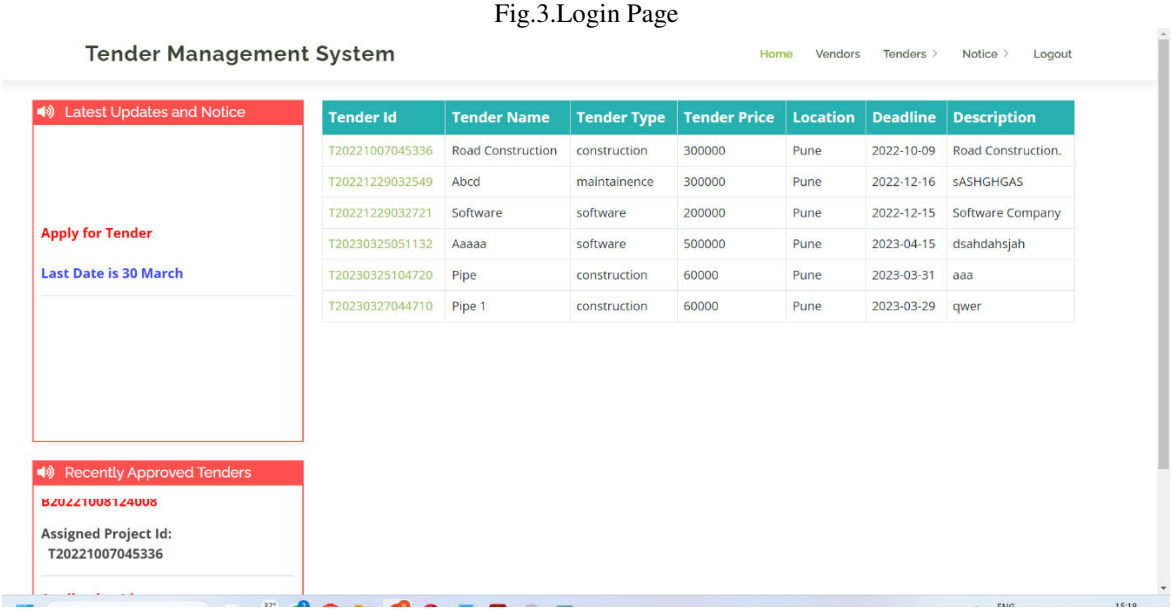

Fig.4. View Tender

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104139 |

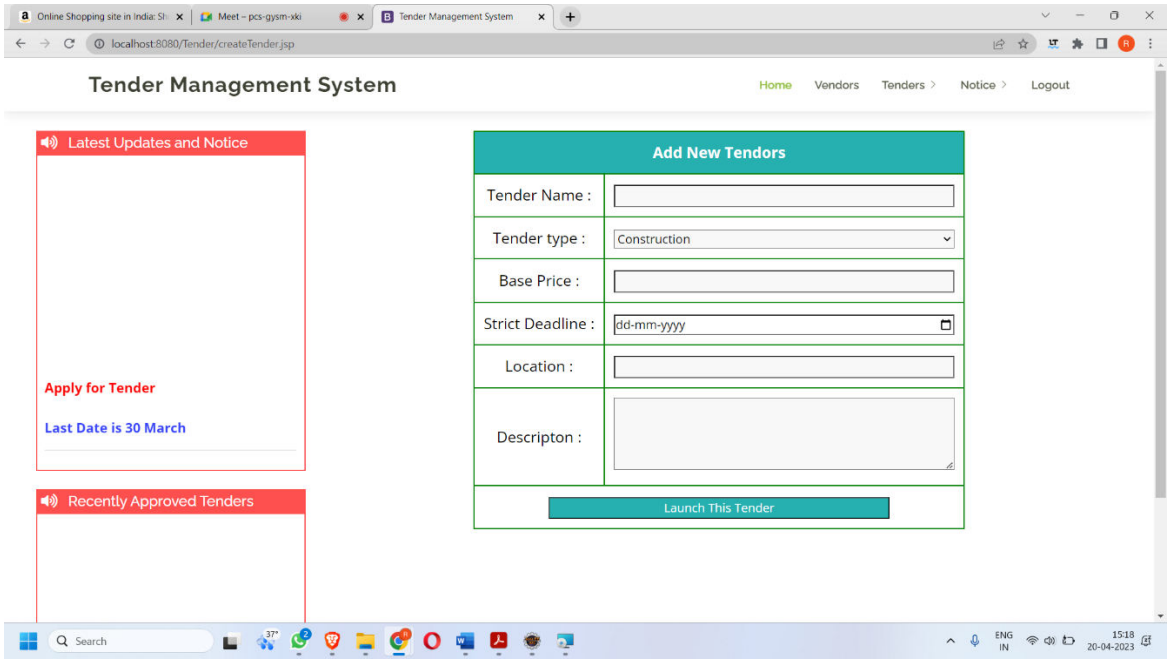

Fig.5.Add New Tender

VI. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs better with the total transmission energy metric than the maximum number of hops metric. The proposed algorithm provides energy efficient path for data transmission and maximizes the lifetime of entire network.As the performance of the proposed algorithm is analyzed between two metrics in future with some modifications in design considerations the performance of the proposed algorithm can be compared with other energy efficient algorithm. We have used very small network of 5 nodes, as number of nodes increases the complexity will increase. We can increase the number of nodes and analyze the performance.

REFERENCES

1. K. C. Davis, “The information act: A preliminary analysis,” The University of Chicago Law Review, vol. 34, no. 4, pp. 761–816, 1967.
2. Ambegaonker, Ajeenkkya, Utkarsh Gautam, and Radha Krishna Rambola. "Efficient approach for Tendering by introducing Blockchain to maintain Security and Reliability." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.
3. Pal, Om, and Surendra Singh. "Blockchain Technology and Its Applications in E-Governance Services.“
4. Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE international congress on big data (BigData congress). IEEE, 2017.
5. Pilkington, Marc. "Blockchain technology: principles and applications." Research handbook on digital transformations. Edward Elgar Publishing, 2016.
6. Wang, Wenbo, et al. "A survey on consensus mechanisms and mining strategy management in blockchain networks." IEEE Access 7 (2019): 22328-22370.
7. Cachin, Christian, and Marko Vukolić. "Blockchain consensus protocols in the wild." arXiv preprint arXiv: 1707.01873 (2017).
8. L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016, pp. 254–26
9. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi,G.Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote,N. Swamy et al., “Formal verification of smart contracts: Short paper,”in Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security. ACM, 2016, pp. 91–96.
10. Wood, Gavin. "Ethereum: A secure decentralisedgeneralised transaction ledger." Ethereum project yellow paper 151.2014(2014): 1-3

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details