Migration Letters

Volume: 21, No: S7 (2024), pp. 65-72

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Blockchain-Based Oversight For Government Tender Processes

[1]Vishal R, [2]Rithick K J, [3]Yagul E , [4]Ms.Viraja Ravi

Abstract

The government has recently released a tender announcement aiming to fulfill the needs of the general public, along with providing information about Earnest Money Deposit (EMD). Unfortunately, the broader public has not been adequately informed about the tender particulars. Bidders are not complying with the terms and conditions outlined in the bidding schedule. Consequently, the performance of the government-appointed agent representing the bidders is causing dissatisfaction among the general public. In an effort to tackle these concerns, we have selected this project. The research focuses on conducting a comparative analysis of the oversight process employed by the government in selecting a reliable agent or company to fulfill the public's requirements through the tendering process. The objective is to prevent activities like DDoS and MitM attacks by securing the tender details within a system. Failure to address this issue may result in corruption and other undesirable activities.

Keywords: *Blockchain, Tender, Bidding, DDOS Attack.*

I INTRODUCTION

This proposed concept leverages blockchain technology to ensure transparency and trust among all stakeholder[1]s involved in the tendering processes network. The implementation incorporates algorithms such as AES and SHA-256 to secure the terms and conditions of the tender stored by the government in the cloud. AES is applied for encrypting and decrypting data within cloud storage, while SHA-256 (Secure Hash Algorithm) is utilized for hashing the dataset using ASCII (American Standard Code for Information Interchange) and the database's Transmission identity document. JSP (Jakarta Server Pages) and Servlet are employed for the front-end, while MySQL serves as the backend.

The entire system comprises three modules: the admin module, the agent module, and public reviews. The Admin Module enables government authorities to manage agent information, input tender data, and view tenders allocated by the system. In the Agent Module, government officers can oversee tenders and submit plan estimates. Agents have the capability to upload plan details and adjust the projected cost on their end. The Public Reviews Module permits users to access information about tenders and their approvals. Users can also submit reviews for each tender, with control over public tender and agent reviews resting in the hands of the administrator.

Therefore, the proposed project aims to support government authorities in choosing the suitable entity to fulfill the task in alignment with the requirements of the general public. This endeavor can lead to the establishment of an equitable and transparent tender auctioning and

[1,2,3]Computer Science and Engineering, Sri Krishna College of Technology, kovaipudur, Coimbatore

[4]M.Tech, Assistant professor, Department of Computer Science and Engineering, Sri Krishna College of Technology, kovaipudur, Coimbatore.

monitoring system, thereby reducing the potential for corruption and fostering increased confidence in the government procurement process.

II BACKGROUND STUDY

In the work by Philipp Frauenthaler et al. [3], It is emphasized that current blockchain relay systems necessitate the destination blockchain to swiftly validate each relayed block header. This leads to substantial operational expenses in implementing relays between Ethereum-based blockchains, given the computational intensity of on-chain block header validation. In response to these challenges, the authors propose a novel relay approach employing a validation-on-demand pattern coupled with economic incentives. This pioneering approach seeks to markedly diminish the operational expenses involved in operating a relay across Ethereum-based blockchains, with the potential to realize a cost reduction of up to 92%. The newly introduced relay method enables decentralized interoperability between various blockchains, including but not limited to Ethereum and Ethereum Classic [3].

According to the work by Loi Luu et al. [6], cryptocurrencies, including Bitcoin and 250 other alternative coins, operate on a blockchain system. This system allows a decentralized network of computer nodes to reliably achieve consensus on a predetermined set of new transactions. Designing a secure blockchain protocol presents a significant challenge, particularly in addressing an ongoing security concern: the creation of a highly scalable consensus process that withstands manipulation y nodes that are Byzantine or arbitrarily malicious. Although Bitcoin's blockchain consensus system is secure, its scalability is constrained, regardless of the available processing.

In this study, we introduce ELASTICO, a novel distributed consensus system designed for permissionless blockchains. ELASTICO demonstrates a nearly linear scaling of transaction rates based on the available mining computation—more computing power in the network corresponds to an increased selection of transaction blocks per unit time. The system is proficient in network messaging and exhibits resilience against byzantine adversaries, tolerating up to one-fourth of the total processing power [6].

Hai Jin, Xiaohai Dai, and Jiang Xiao [7] highlight that the upcoming ecosystem will be powered by a diverse array of blockchain systems. The success of these systems is increasingly dependent on effective cross-chain collaboration to enhance features and capabilities in the evolving landscape. The challenge lies in achieving 'interoperability'—ensuring seamless communication and efficient data transmission across various blockchain systems, a task fraught with both theoretical and practical challenges. This work begins by elucidating the concept of interoperability, emphasizing its interdisciplinary nature. Subsequently, it outlines a roadmap that identifies obstacles requiring resolution for achieving interoperability. Lastly, the paper introduces innovative architectural techniques aimed at bridging the gap by promoting interoperability across multiple levels of blockchain systems [7].

Abdallah Qusef et al. [8] discuss the ongoing revolution in information technology solutions and the widespread transition from traditional manual procedures to automated and digital workflows. In reaction to this transformation, a range of electronic solutions has been created and utilized to digitize processes within the supply chain. Given the significance of procurement within the supply chain, there is a growing demand for enterprises to conduct procurement activities through an e-procurement system. This paper specifically underscores the importance of transitioning an enterprise's tendering process into a fully electronic format by implementing the e-Tendering strategy as an integral part of e-Procurement.

This study presents a novel e-Tendering model that allows organizations to execute a completely automated tendering process through a web-based platform. The proposed model encompasses a groundbreaking conceptual framework for a comprehensive digital tendering solution, implemented through a web-based platform. It encompasses every stage of the

tendering process and integrates pertinent modules from departmental computer systems, along with involving stakeholders. Additionally, it suggests a fresh approach to involve bidders in the e-Tendering system, establishing a complete digital cycle for the entire tendering process. Addressing a significant challenge in current e-Tendering solutions, which often rely on manual paperwork, this model aims to bring the tendering process up to speed with the digital environment prevalent today [8]. This idea can be employed to establish a novel framework for developing a suitable e-Tendering system that completely automates the tendering process within any enterprise's TMS.

Yashita Goswami, Ankit Agrawal, and Ashutosh Bhatia [10] highlight the growing prevalence of e-governance, involving the use of information technology for government tasks like service delivery and information exchange. E-tendering is a notable example of e-governance, contributing to enhanced efficiency in the tendering process. However, despite these improvements, there exists a trust imbalance between citizens and the government due to the centralized control of the entire tendering process. Various research studies suggest exploring decentralized approaches to enhance the security, transparency, and fairness of e-tendering.

Presently, the government publicly communicates the challenges and issues they are addressing, expressing a desire for input from residents to enhance problem-solving. This article introduces a strategy based on permissioned blockchain to establish a transparent and equitable tendering system, incorporating active citizen participation and fund tracking. The proposed method enables citizens to observe the tendering processes transparently, offer suggestions and solutions for addressing the government's stated concerns, and receive due recognition for their contributions [10].

III PROBLEM DEFINITION

Government tender processes are crucial for allocating public resources and ensuring fair competition among vendors. However, traditional tender monitoring systems often face challenges related to transparency, accountability, and susceptibility to fraud. The lack of a tamper-resistant and transparent system can lead to corruption, inefficiencies, and disputes in the procurement process. Current tender processes lack transparency, making it difficult to trace and verify the entire lifecycle of a tender, from issuance to contract award. The centralized nature of existing systems exposes them to the risk of data tampering, leading to fraudulent activities such as bid manipulation and document forgery. Implementing a blockchain-based system for government tender monitoring can address these challenges by providing a transparent, secure, and immutable ledger for the entire tender lifecycle. Use blockchain to establish and verify the identities of participating entities, ensuring that only authorized and qualified bidders participate in the tender process.

IV PROPOSED MODEL

The proposed government tender monitoring system harnesses blockchain technology to elevate transparency, security, and accountability in the procurement process. Through a decentralized and immutable ledger, the system guarantees the secure recording of all tender-related transactions, spanning from the initial bidding phase to contract awards, with transparent accessibility for pertinent stakeholders. Smart contracts play a crucial role in automating and enforcing predefined rules, diminishing the risk of fraud and corruption. Furthermore, blockchain implementation bolsters data integrity, preventing unauthorized modifications to tender information. This innovative solution cultivates trust among participants, streamlining the tendering process and ultimately contributing to a more efficient and equitable public procurement system. The SHA-256 algorithm is employed to encrypt data saved in the cloud, presenting the selected agent to the admin in the form of encrypted data.

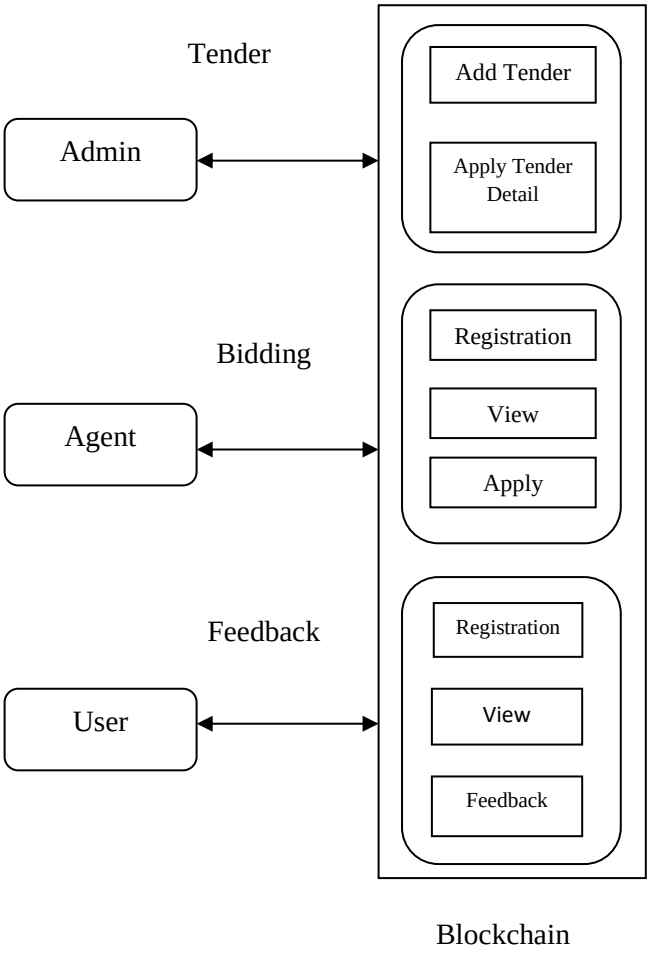

Fig.1.System Architecture

V RESULTS AND DISCUSSION

The consecutive flow of work in the aimed e-tendering based on blockchain is outlined as follows:

1) The admin enrolls individuals, tendering companies, and auctioneer to enable their engagement with the network.
2) Once activated, the provided business card allows them to interact with the network.
3) Subsequently, the bidding agent accesses the tender specifications from the blockchain network.
4) Companies are allowed to submit their bids for a tender only after the tender has been initiated and before the specified tender deadline.
5) The submitted auction bids are evaluated on the network using the established business logic.
6) The announcement of the winner takes place following the tender proposal deadline, adhering to the business rules.

5.1 Cryptographic hash function:

SHA-256 serves as a cryptographic hash function, transforming text of varying lengths into an almost-unique alphanumeric string consisting of 256 bits. It plays a crucial role in prominent blockchain protocols such as Bitcoin and Bitcoin SV. In the Bitcoin blockchain, SHA is integral

to implementing the proof-of-work (PoW) consensus algorithm. Additionally, SHA is employed to convert user passwords into a hash value before being stored in a database.
SHA-256, short for Secure Hash Algorithm 256-bit, is a cryptographic hash function that falls under the SHA-2.
The input message undergoes padding to ensure that its length is a multiple of 512 bits (equivalent to 64 bytes).
The padding process involves adding a solitary '1' bit, succeeded by '0' bits, and concluding with the representation of the original message length in bits (expressed as a 64-bit integer).

5.2Formulas and Operations:
SHA-256 uses several logical and bitwise operations, including AND, OR, XOR, NOT, modular addition (mod 2^32), and circular shifts.

Ch Function:
$Ch(x,y,z)=(x \wedge y) \oplus (\neg x \wedge z)$

Maj Function:
$Maj(x,y,z)=(x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$

Sigma Functions:
$\sigma 0(x)=(ROTR2(x)) \oplus (ROTR13(x)) \oplus (ROTR22(x))$
$\sigma 1(x)=(ROTR6(x)) \oplus (ROTR11(x)) \oplus (ROTR25(x))$

ROTR (Right Rotate) Function:
$ROTRn(x)=(x \ggg n) \oplus (x \lll (32-n))$

NOT, AND, OR, XOR:
¬ denotes bitwise NOT
The symbol ∧ represents a bitwise AND operation.
The symbol ∨ represents a bitwise OR operation.
The symbol ⊕ represents a bitwise XOR operation.
These operations are used within the message processing steps and are combined with the message schedule and round constants to update the hash values.

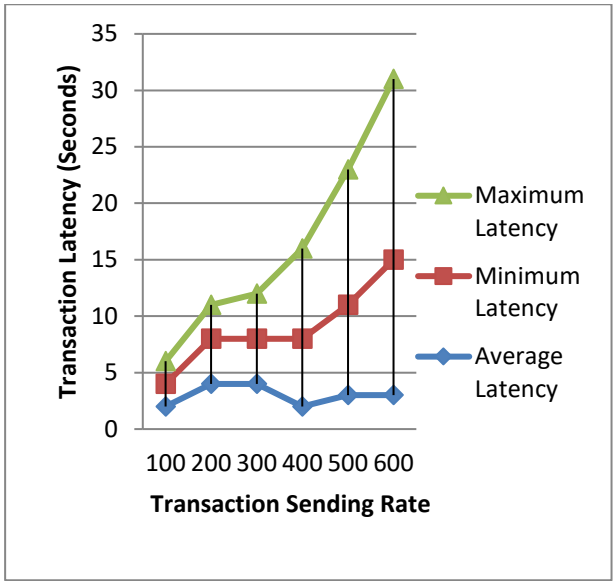

Fig.2.Latancy and Transaction Rate

In this project, we examined the highest, median, and lowest transaction latencies during multiple runs of our experiments. As the throughput reached 100 TPS, the maximum delay increased, while the minimum latency consistently remained below 1 second.

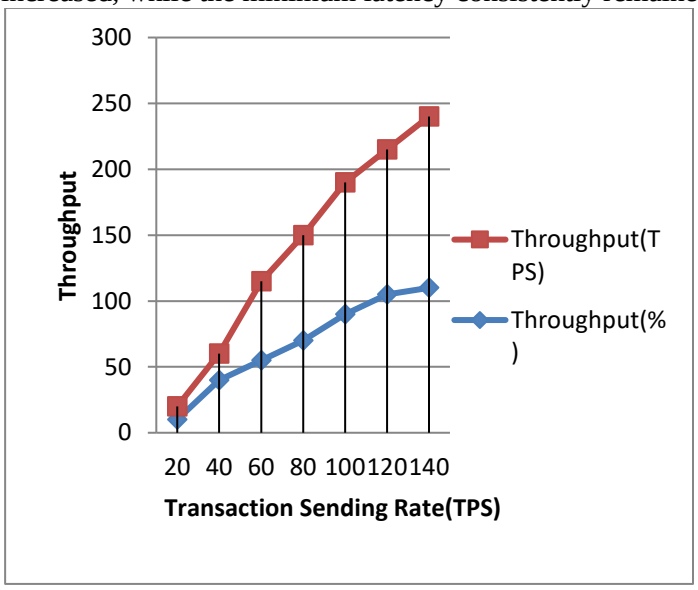

Fig.3. Throughput

The throughput remained steady at approximately 100%, even when the sending rate reached its maximum of 110 TPS. This stability persisted even with the elevated sending rate of 110 TPS.

VI CONCLUSION AND FUTURE WORK

In conclusion, implementing government tender monitoring using blockchain technology holds great potential for enhancing transparency, efficiency, and security in the procurement process. The decentralized and immutable nature of blockchain ensures that the data related to tenders is secure, transparent, and tamper-resistant. This can significantly reduce corruption, fraud, and

errors in the tendering process, leading to fair competition and better outcomes for both the government and participating businesses. Through the utilization of smart contracts, the execution of tender-related activities can be automated, lessening reliance on intermediaries and reducing the likelihood of human errors. Additionally, stakeholders involved in the tendering process, such as government officials, contractors, and auditors, can benefit from real-time access to a single version of the truth, improving collaboration and trust.

While the potential benefits of implementing government tender monitoring using blockchain are substantial, there are areas for further research and development to enhance the effectiveness of such systems. Explore ways to improve the ease of use blockchain networks to handle the large volume of transactions associated with government tendering processes, ensuring efficient and timely processing. Address concerns related to privacy and confidentiality, especially in sensitive information handling during the tendering process. Implementing privacy-focused solutions on the blockchain can be crucial for compliance with data protection regulations. Explore synergies with other emerging technologies, such as AI, IoT, and ML, to create more advanced and intelligent government tender monitoring systems.

Reference

[1] A. Mizrahi, N. Koren, and O. Rottenstreich, "Optimizing Merkle proof size for blockchain ransactions," in Proc. Int. Conf. COMmun. Syst. NETw. (COMSNETS), 2021, pp. 299–307.
[2] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in Advances in Cryptology (CRYPTO), J. Katz and H. Shacham, Eds. Cham, Switzerland: Springer Int., 2017, pp. 357–388.
[3] P. Frauenthaler, M. Sigwart, C. Spanring, M. Sober, and S. Schulte, "ETH relay: A cost-efficient relay for Ethereum-based blockchains," in Proc. IEEE Int. Conf. Blockchain (Blockchain), 2020, pp. 204–213.
[4] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in Proc. IEEE Symp. Security Privacy (SP), May 2018, pp. 315–334.
[5] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta,and B. Ford, "OmniLedger: A secure, scale-out, decentralized ledger via sharding," in Proc. IEEE Symp. Security Privacy (SP), 2018, pp. 583–598.
[6] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 17–30. [Online]. Available: https://doi.org/10.1145/2976749.2978389.
[7] H. Jin, X. Dai, and J. Xiao, "Towards a novel architecture for enabling interoperability amongst multiple blockchains," in Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS), 2018, pp. 1203–1211.
[8] Qusef, A., Daradkah, M., Sammour, G., & Albadarneh, A. (2019, December). A New e-Tendering Model For Fully Automated Tendering Process. In 2019 International Arab Conference on Information Technology (ACIT) (pp. 193-201). IEEE.
[9] Yutia, S. N., & Rahardjo, B. (2019, November). Design of a blockchain-based e-tendering system: a case study in LPSE. In 2019 International Conference on ICT for Smart Society (ICISS) (Vol. 7, pp. 1-6). IEEE.
[10] Goswami, Y., Agrawal, A., & Bhatia, A. (2020, December). E-governance: A tendering framework using blockchain with active participation of citizens. In 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1-4). IEEE.
[1] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 270–282. [Online]. Available: https://doi.org/10.1145/2976749.2978326.
[12] "Community alert: Ronin validators compromised." Ronin Network. 2022. Accessed: Sep. 8, 2022. [Online]. Available: https:// roninblockchain.substack.com/p/community-alert-ronin-validators.
[13] Ateniese, G., Bonacina, I., Faonio, A., Galesi, N.: Proofs of space: when space is of the essence. In: Abdalla, M., de Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 538–557. Springer, Cham (2014). doi:10.1007/978-3-319-10879-7 31

[14] Aumann, Y., Lindell, Y.: Security against covert adversaries: efficient protocols for realistic adversaries. J. Cryptol. 23(2), 281–343 (2010)
[15] Bentov, I., Gabizon, A., Mizrahi, A.: Cryptocurrencies without proof of work. CoRR, abs/1406.5694 (2014)