IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Smart Contract Allocation System Using Blockchain With Auction System

[1]Naziya M.Hanif Pathan
[2]Nagnath S Bagal
[3]Ganesh S. Wayal

Department of Computer Science and Engineering, PVPIT, Bavdhan , Pune, India

***Abstract*—** Nick Szabo first used the phrase "smart contract" in 1994 to describe a software that may be programmed to carry out any task upon the satisfaction of certain predetermined criteria. Nick Szabo first used the phrase "smart contract" in 1994 to describe a software that may be programmed to carry out any task upon the satisfaction of certain predetermined criteria. Globally, public sector organizations and governments are always exploring innovative approaches to stay abreast of technological developments in order to attain cost optimization, work efficiency, and smart governance.

One such method that has drawn interest from governments all around the world in recent years is blockchain technology. The blockchain can expand to another province thanks to low-cost methods, increased traceability, and enhanced security. Governments typically award contracts to private companies for various projects.

Different rivals attempt to keep an eye on one other's tender values during this procedure in an effort to secure the contract. In order to approve the deal in recognition of a particular third party, the callous government officials also accept large bribes. In this initiative, we want to use blockchain technology to create a transparent and safe mechanism for allocating government contracts. Government documents that are very vulnerable to manipulation are stored on blockchain, which is a reliable and immutable data format.

***Index Terms*— Blockchain, Edge Computing, Smart Contracts, Contract Allocation,Edge Computing,Bid,Auction System,Firebase**

I. INTRODUCTION

The application of blockchain technology has grown quickly worldwide and in nearly every industry. To improve security, privacy, transparency, and workflow efficiency in the government contracting process, blockchain technology presents a very promising alternative.

Blockchain enables all parties to a given contract to be a part of the same network and to keep an eye on the workflow in real time [1]. Governments around the world, including those in Georgia, the UK, the UAE, Australia, China, Japan, and Russia, are now integrating blockchain technology into their daily operations at a very quick speed. The administration of Dubai has an ambitious objective of becoming entirely paperless through the dissemination.

Smart contracts have garnered significant interest and have been implemented across various industries to facilitate more streamlined and reliable transactions. As of August 2018, the total market value of cryptocurrency was valued at over 200

billion US dollars. [2]. In recent years, the governments of some developing nations, including India, have also supported a variety of initiatives and regulations for the adoption of blockchain technology. [3].

Numerous initiatives have been made to use technology to make government procedures quick and paperless. Examples of these initiatives include online tax return filing, online ticketing systems, and

online contract issuance. Even if the majority of these systems appear reliable and well-designed, they are all predicated on the notion of a single point of failure—a central server—because hackers may readily compromise it or interfere with its operation by launching attacks like denial-of-service, slow-loris, SYN flooding, etc.[4]. In most governments, complicated bureaucratic systems often result in highly inefficient work-flow fraught with corruption, mismanagement, and human errors. Some of the governance processes, such as government contracts include malpractices like information leaks, corruption, bribery, etc. Most of the existing electronic services and IT infrastructure have the above-mentioned limitations, however, new technologies such as blockchain have the potential to greatly ameliorate the existing problems [5], [6]. A permissioned blockchain network can provide the necessary transparency to effectively implement government policies for the benefit of the citizens of the country and fix responsibilities in case of abuse of the system [7], [8]. Blockchain is used as a stable and unchangeable data structure to store the government records that are highly susceptible to interfere.

In the current digital space, data manipulation is one of the most important tools that is being used by all the adversaries and malicious entities to cause harm to the public and the government bodies [9]. Most of the existing systems rely on the data and if the data itself is far given correlated or misreported, then the complete system becomes corrupt. The shift from storing data in physical files to storing data in digital form is a paradigm shift [10]. However, if the digital data is not secure, then the harm caused by the loss of digital data would be much more than the harm that was faced due to the loss of physical files [11]. According to 2019 statistics, there are more than 130 large-scale targeted data breaches in the U.S. per year, and that number is growing by around 27 percent per year. Digital Identity theft is one of the major sources of data breaches. It is estimated that 74% of the data breaches are caused by identity thefts across the world. The United States leads other countries with almost 85 percent of digital identities stolen worldwide [12].

In addition to data breaches, another problem that is unique to government operations is bribery and needless delays in the procedures. Government representatives frequently abuse their bureaucratic authority and demand large bribes in order to get contracts approved.

Our goal in this paper is to address these problems and create an open, safe, and edge computing infrastructure for government contract allocation that not only does away with the need for human oversight or intervention but also makes it simple for the government to monitor and update its policies over time. In order to address this problem, we provide a framework that makes use of blockchain technology to establish a decentralized system that facilitates easy, transparent, auditable, and unchangeable government tendering procedures.

This is how the remainder of the paper is structured. Section II contains the most recent research on employing emerging technology to improve office workflow in relation to government contracts and other areas. Section III provides some background information on blockchain technology. An overview of the system is given in Section IV. Section V presents the suggested architecture, the smart contracts in use, and the best possible price calculation. The simulation findings are shown in Section VI, and the paper is ultimately concluded in Section VII.

II. Related Work

Regretfully, there is a dearth of research on blockchain applications in the government sector, with relatively few papers specifically covering the subject. This suggests that there is a disconnect in the adoption of Blockchain technology between applications connected to government and the remaining major fields of study. As a result, blockchain technology is becoming more and more interested in government contracts [13]. In [14], Joe Abou et al. go over the several application cases and industries that are currently utilizing blockchain technology.

The potential and advantages of leveraging blockchain technology to lower the time and effort needed to manage and maintain government tasks have been further discussed by the authors of [15]. The use of smart contracts is presented as a potential remedy to stop bribery and corruption in government office operations. Additionally, they significantly cut down on the time needed to finish a task, launch new services, and improve the residents' Quality of Service (QoS). Blockchain technology has been proposed by Svein et al. [16] as a means of enhancing citizen-government transparency. To improve overall fairness, the data can be made anonymous and the entire transaction can be audited and tracked.

In order to raise the general caliber of the credit system, authors of [17] have suggested using the unchangeable properties of blockchain technology and storing financial data there. The Chinese wall approach was put forth by the authors of [18] in an effort to reduce

fraud in the government contracting process. The e-procurement policies in Tanzania that have led to an effective e-contracting system were presented by Amani Dello et al. [19]. The authors of [20] outline the issues facing China's bidding market and suggest using an e-contract as a model for a bidding platform to address these issues. The approach put forth by Hiroshi Fukui et al. [21] involves assigning a government contract to a contractor based on a variety of factors, including cost, quality, timeliness, and so forth.

One of the main topics that has received a lot of attention lately is identity management. The authors of [22], [23], and [24] have put forth a number of blockchain-based frameworks and techniques to create a safe, unique, and unchangeable identity for every citizen. A number of safe electronic voting options are put up in [25] to facilitate a simple and safe voting process. Because blockchain technology is decentralized, there is less chance that one rogue centralized authority can jeopardize the voting process. A blockchain-based approach for government information exchange and administration has been put forth by the authors of [26].

The general interest of the government and constructors is not taken into consideration, despite the few recent attempts to develop a decentralized application for the government contract procedure. The main goal of the suggested framework is to improve government officials' and constructors' overall experience. The goal of the suggested architecture is to build an end-to-end edge computing framework in which all parties can function as members of the same network and official activity can proceed in an entirely impartial and transparent manner.

III. BACKGROUND

A blockchain is a distributed database, or public ledger, that is shared by several network participants and contains records or transactions. In light of this, a blockchain can be classified as either permission-less (public) or permissioned (private), depending on whether or not users are able to join the network at will [27]. Anyone can take part in the transaction validation process on a permission-less blockchain network if they are given a special address to use to communicate with the network, similar to Bitcoin. Users are unable to join the network, see the recorded ledger, or freely issue transactions on a permissioned blockchain, which is a closed environment [28].

The majority of businesses avoid using permissionless blockchain due to two main disadvantages: the transaction history is publicly viewable and achieving consensus needs a significant amount of processing power [29]. Conversely, the permissioned blockchain restricts the parties that are able to transact on the network, which in turn limits the general public's ability to participate. As a result, we employ consor- tium blockchain, which benefits from the advantages of both networks [30]. While transactions are only validated by authorities and co-authorities, common constructors or construction companies are permitted to join the network by providing their legitimate IDs. Therefore, a consortium blockchain offers an additional layer of privacy while also having all the key benefits of a permission-less network [31].

Ethereum is one such platform that enables the development of distributed applications. It is an open-source cooperative effort made to progress blockchain technology across industries. Leading figures in banking, supply chains, technology, supply chains, finance, and the Internet of Things are involved in this global partnership, which is being facilitated by The Linux Foundation. Apart from the blockchain, Ethereum's ability to smoothly integrate Smart Contracts into the network is its most significant feature. Additionally, it permits the establishment of specific Private Channels that have the capacity to retain a record of a different ledger that is only accessible by channel users.

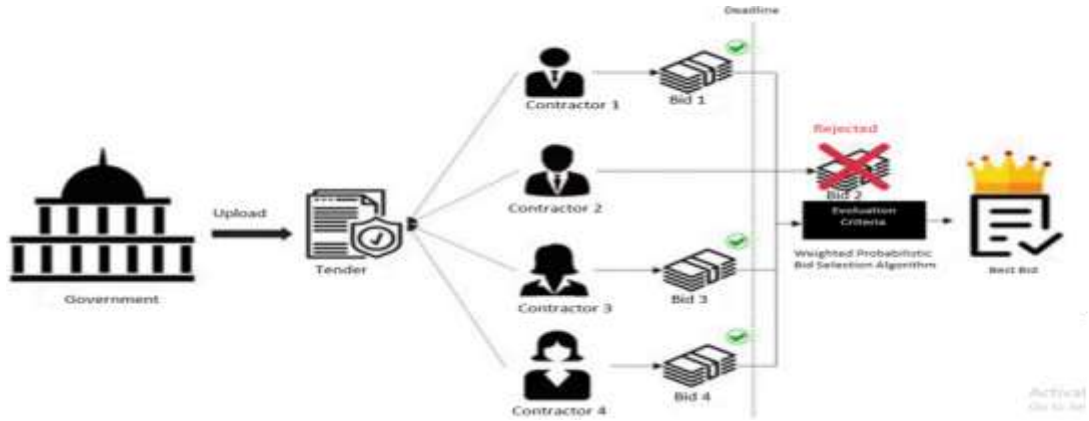

Fig. 1: Implementation of the Proposed System

IV. Proposed Model for Government Contracts

Fig. 1 shows the steps involved in the allocation of tenders from government lenders to constructors. In the beginning, government lenders and builders join the blockchain network to build a safe infrastructure for edge computing. All relevant constructors receive the tender details from the government lender. Additionally, there is a double auction between the government lenders and the constructors.

Ultimately, the constructor who submitted the lowest bid is given the contract. A decentralized consortium architecture that combines the openness and transparency of a permission-less blockchain with the security and privacy of a permissioned blockchain makes up the suggested paradigm. The model's goal is to securely and effectively manage the government tendering process. Three primary categories of entities comprise the system: government officials, external entities such as building corporations or individual builders, and banks. Ethereum allows us to regulate network nodes' access to data using identity identification. The files are only accessible to the nodes that are authorized to examine or validate the specific data.

A. Smart Contract Design

Legally binding contracts known as "smart contracts" are made with operational parameters linked to a standard programming language. A smart contract is implemented to guarantee that the until all nodes correctly verify and label a transaction as complete, it will not be added to the block. Following verification, the transaction information, timestamp, and participant public key will be added to the blockchain and the final transaction log. A set of key-value pairs that are recorded on the ledger and saved on the blockchain are the outcome of smart contracts that are carried out via transaction proposals.

B. Decentralized Document Storage

A three-layer file encryption architecture is developed since the majority of transactions typically involve many document kinds that must be processed. This enables for the hassle-free and secure decentralized storage of all the documents needed for a given transaction. In addition to

preventing single points of failure, the decentralized architecture of the storage service guarantees speedy network access to updated copies. Let's say Department A needs to send a contract proposal to Department B for finalization. The procedures for moving and storing documents securely are as follows.

• Step 1: Using his private key created with ECDSA, an authorized Dept. A employee will first digitally sign the proposal.
• Step 2: Following signature, the proposal will generate a random 32-byte passphrase and proceed through a Symmetric Encryption (AES-256) stage.
• Step 3: After that, this passphrase will be encrypted using the public key of the Dept. B selected individual using symmetric encryption (RSA-512).
• Step 4: The document will thereafter be added to the decentralized storage and synchronized with every node, where it will await verification by the

smart contract and consensus-based approval from the other nodes.
• Step 5: The proposal will be modified and saved once again following approval and verification.

The above-described procedure employs three layers of cryptographic encryption. The Elliptical Curve Digital Signature Algorithm (ECDSA), which is used in the first layer, ensures the signer's identity in addition to maintaining the file's integrity. While awaiting network approval, the file is encrypted by the Second Layer using AES-256 to prevent tampering. To ensure that only the intended recipient has access to the file, the third tier encrypts the passphrase created by the second layer using RSA-512 and the recipient's public key.Members of that specific channel can see and understand the entire work-flow. The adversaries who attempt to intentionally postpone the duties for immoral reasons will be demotivated by this openness. Additionally, the flow will assist in highlighting the network's harmful nodes. Because blockchain technology is immutable, even while anybody in the channel can see the transactions, no one can change their status.

V. CONCLUSION

The necessity and advantages of applying blockchain technology to the government contract assignment procedure have been covered in detail in this study. The end-to-end edge computing infrastructure for government contract work-flow has been implemented using Ethereum.The best constructors are linked to the contract projects using an iterative auction procedure.

REFERENCES

[1] Nick Szabo. Smart contracts, 1994.

[2] CoinMarketCap. Cryptocurrency total market capitalization, Au- gust 2018.

[3] "Blockchain for government services—use cases, security benefits and challenges," A. Alketbi, Q. Nasir, and M. A. Talib, at the 15th Learning and Technology Conference (L&T) of 2018. 2018 IEEE, pp. 112-119

[4] According to coindesk, "A national framework to facilitate the broader implementation of blockchain use cases is being developed by the Indian government." India intends to release a national blockchain architecture, according to an internet source on November 27, 2019.

[5] In IEEE Access, vol. 7, pp. 25 086–25 086, 2019, H. Cho wrote a correction to asic-resistance of multi-hash proof-of-work techniques for blockchain consensus protocols.

[6] A blockchain-based architecture for lightweight data sharing and energy trading in v2g networks, V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, IEEE Transactions on Vehicular Technology, 2020.

[7] A distributed architecture for energy trading between uavs and charging stations for critical applications, V. Hassija, V. Chamola, D. N. G. Krishna, and M. Guizani, IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5391–5402, 2020.

[8] Hyperledger fabric: a distributed operating system for permissioned blockchains, E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Proceedings of the Thirteenth EuroSys Conference. ACM, 2018, page 30.

[9] Dagiov: A framework for vehicle-to-vehicle communication utilizing divided acyclic graph and game theory, V. Hassija, V. Chamola, G. Han, J. J. Rodrigues, and M. Guizani, IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4182–4191, 2020

[10] "Smart contract templates: essential requirements and design options," C. D. Clack, V. A. Bakshi, and L. Braine, arXiv preprint arXiv:1612.04496, 2016.

[11] Cachin, C. "Architecture of the hyperledger blockchain fabric," in Workshop on Consensus Ledgers and Distributed Cryptocurrencies, vol. 310, 2016.

[12] H. Cho, "Multi-hash proof-of-work mechanisms for blockchain consensus protocols: asic-resistant," IEEE Access, vol. 6, pp. 66 210–66 222, 2018.

[13] "The History of Data Breaches," by J. D. Groot. Oct. 24, 2019, online at https://digitalguardian. com/blog/history-data-breaches.

[14] IEEE Communications Surveys Tutorials, vol. 20, no. 3, pp. 2543–2585, third quarter 2018, M. C. Kus Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems."

[15] J. A. Jaoude & R. G. Saade, "Usage of blockchain applications in various domains," IEEE Access, vol. 7, pp. 45 360–45 381, 2019.

[16] H. Hou, "Blockchain technology's application in China's e-government," in the 26th International Conference on Computer Communication and Networks (ICCCN), 2017. pp. 1-4, IEEE, 2017.

[17] International Conference on Electronic Government, "Blockchain technology as a support infrastructure in e-government," S. Ølnes and A. Jansen. 2017 Springer, pp. 215–227.

[18] S. Ølnes, International Conference on Electronic Government, "Beyond bitcoin enabling smart government using blockchain technology." Springer (2016)

[19] S. Ølnes, International Conference on Electronic Government, "Beyond bitcoin enabling smart government using blockchain technology." 2016 Springer, pp. 253-264.

[20] "Information confidentiality and the Chinese wall model in government tender fraud," by S. Rama, S. V. Flowerday, and D. Boucher, Information Security for South Africa, 2012. 1-8 in IEEE, 2012, pp.

[21] 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD), 2017; A. Dello and C. Yoshida, "Online tendering and evaluation for public procurement in tanzania." 2017; IEEE, pp. 137–141.

[22] In the 2011 International Conference on Internet Technology and Applications, Z. Hui and J. Yang presented their research on the use of e-tender in China. 2011 IEEE, pp. 1-3.

[23] "Optimal comprehensive tendering models for project procurement," by H. Fukui and K. Kobayashi, in the 2010 IEEE International Conference on Systems, Man, and Cybernetics. 2010 IEEE, pp. 3258–3264.

[24] P. Dunphy & F. A. Petitcolas, "A preliminary examination of blockchain-based identity management schemes," IEEE Security & Privacy, vol. 16, no. 4, pp. 20–29, 2018.

[25] An id-based linearly homomorphic signature method and its application in blockchain was published in IEEE Access, vol. 6, pp. 20 632–20 640, 2018, by Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang.

[26] "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," by C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo IEEE Access, volume 6, 2018, pages 28 203–28 212.

[27] P. Noizat, "Electronic voting on a blockchain," in Digital Currency Handbook. 2015 Elsevier, pp. 453–461.

[28] "Research on government information sharing model using blockchain technology," Y. Zhang, S. Deng, Y. Zhang, and J. Kong, in the 2019 10th International Conference on Information Technology in Medicine and Education (ITME). 2019 IEEE, pp. 726–729.

[29] P. Dunphy and F. A. P. Petitcolas, "A preview of blockchain-based identity management systems," IEEE Security Privacy, vol. 16, no. 4, July 2018, pp. 20–29.

[30] Blockchain-enabled smart contracts: Architecture, applications, and future trends, S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, IEEE Transactions on Systems, Man, and Cybernetics: Systems, pp. 1–12, 2019.

[31] Low-cost digital signature architecture appropriate for radio frequency identification tags, M. O'Neill and M. J. B. Robshaw, IET Computers Digital Techniques, vol. 4, no. 1, pp. 14–26, January 2010.