IPEC Journal of Science & Technology, Vol. 01 (02), Oct. 2022

ISSN: 2583-3286(Online)

Smart Contracts through Block-chain

Krishna Kumar, Rishabh Arora, Sarthak Saini, Shubham Bisht, Yatin Singhania
Department of Information Technology, Inderprastha Engineering College, Ghaziabad, Uttar Pradesh, India

Abstract: **This article outlines of study on smart contracts using block chain technology. Block chain technology integrated into the railway tendering system to make the process more efficient and transparent for bidders. From both ends, this project will benefit the railway and the contractors. This paper will go through railway contracts in detail, as well as block chain, ethereum, and solidity. It also provides a quick overview of how tenders were filled out in the offline process, as well as the procedure. To make the process transparent, smart contracts deployed in the railway tender system. There was a lot of poll (corruption) in the system at first, thus it was necessary to eliminate the middleman problem in the tender process. Because of block chains decentralized structure. When transactions are recorded, the record does not belong to a single entity. All relevant parties have access to the data and can observe when and how a payment or value transfer was completed. Main objective of work is to cut out the middleman and the time it takes to return the earnest money that is paid when the tender is filled out. In circumstances when contract conditions may be seen openly, smart contracts can help by removing the intermediaries. Using block chain technology, these contracts increase trust and transparency between two parties. Smart contracts are beneficial since they are cost-effective and time-saving, as well as secure and precise. The conclusion of research is that the process of awarding contracts to contractors has been moved online, using block chain technology, from a manual procedure. As the process moves to the internet, it automates and integrates the buyer and supplier processes. From tender preparation to purchase order, invoicing, and electronic payment, it automates the entire procurement process.**

Keywords- **Block chain, Ethereum, Payments, Smart contracts, Supply chain, Solidity**

I. INTRODUCTION

Current Offline & E-Tendering methods aren't 'fair and open,' which means that information isn't shared with all stakeholders (Right to Information). For example, when a firm is chosen as the winner of a contract, other companies that bid on the same tender are not informed of why their bid was rejected and why a particular company was chosen as the winner. A corporation can request this information, but obtaining it is a time-consuming process. Despite the fact that checking these papers is possible, analyzing them takes time. Apart from not being transparent, these portals' security is a big concern, leading to fraud and data tampering in a centralized database. Because it focuses largely on decentralization of information and is secured by encryption integrated with indisputable block-based architecture for transaction management, block chain technology can be utilized to address these security concerns. As a result, Block chain and Smart Contracts can be utilized to create a transparent, decentralized, and secure tendering framework that allows bidders to monitor portal functionalities and track all of the tender portal's activity. Governments and businesses commonly use the tendering process to buy goods or any type of services from manufacturers or service providers.

Date of Submission: 31 May 2022
Date of Acceptance:15 September 2022
Corresponding Author: Rishabh Arora (arorarishu11@gmail.com)

However, because e-tendering is the most widely utilized procurement method, it has a number of security problems. Because it focuses largely on decentralization of information and is secured by encryption integrated with indisputable block-based architecture for transaction management, block chain technology can be utilized to address these security concerns. The use of smart contracts (based on the Ethereum block chain) to construct a distributed e-tendering system is investigated in this study. The issues of security and audibility are assessed and contrasted to the current procurement process. The primary goal of this article is to provide a fair, transparent, and open procurement process.

II. LITERATURE SURVEY

Unfortunately, there is very little study on block chain applications in the government sector, with only a few papers on the subject. This implies a Block chain technology adoption gap between government-related applications and those in other major disciplines of study. As a result, the use of block chain in government tenders is becoming increasingly popular.

- The current tendering mechanism for railways is done manually.
- The railway will first publish a tender. a

  tender document which was issued by the western railways. In the document a few things are mentioned like Name of work, Date of tender submission, Date of tender opening, Approximate cost.

ISSN: 2583-3286(Online)

- The bidder will now purchase the Tender Form, the price of which is determined by the work cost of the tender issued by the railways. Contractors have to fill Name, Money receipt no.(earnest money) and date at which they are filling the tender.
- Let's say the job is worth 5 lakhs rupees. The bidder will submit the tender form along with a 2% earnest money deposit.
- If he/she is assigned, the money will not be returned; otherwise, it will be returned after three months when the work is sanctioned to another bidder.
- Now, the person must now submit a completed paperwork as well as cash to the station manager.
- She or him has two alternatives here: give cash and get a receipt, or issue an FDR in the name of a senior account railway officer from any nationalized bank.
- Then it is sealed, and on the opening day, in front of all the bidders, the railway official opens each packet one by one, and whomever has made the lowest bid receives the tender.
- Consider the following scenario: there are four works (tenders) and four 'thekedars,' thus they communicate with one another and learn who is bidding what, and the tenders are awarded accordingly.
- With the use of smart contracts, there will be more transparency, and because it is a decentralized process, everyone will know who bid what.

III. PROPOSED FRAMEWORK

The steps in allocating tenders from government lenders to contractors are depicted in Figure 3.1. In the beginning, government lenders and builders join the block chain network to build a secure edge computing infrastructure. All relevant constructors are informed about the tender by the government lender. In addition, the constructors and government lenders participate in a double auction. Finally, the tender is assigned to the constructor with the minimum bid. The suggested paradigm is a decentralized consortium architecture that combines the security and privacy of Permissioned Block chains with the openness and transparency of Permission-less Block chains. The model's goal is to handle the government tender procedure

efficiently and safely. Data can regulate access by network nodes using Ethereum based on identity identification. The files are only accessible to nodes who have been granted permission to examine or verify the data in question.

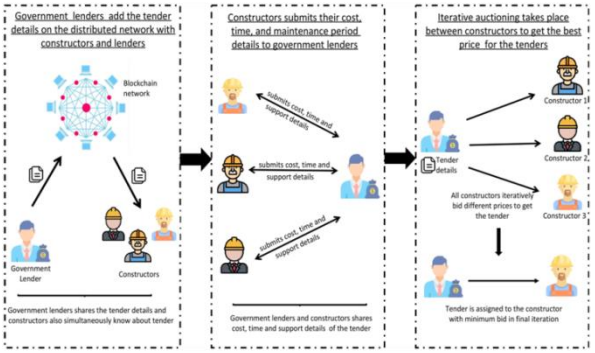

Figure 1. Proposed Framework

IV. SYSTEM DESIGN

1. The tendering organization creates a tender by stating details such as description, bidding period, approximation cost and so on.
   a. Tender stipulation occurs, in which the tendering company defines its requirements as well as the evaluation criteria that will be used to evaluate a proposal.
   b. The tender is then sent to the block chain in the form of a smart contract once the tender details are finished and the documents are provided. Only companies that are willing to bid have access to the documents, which are stored in an encrypted format in a database.
2. The bidder registers with the system asynchronously. The bidder is then presented with a list of all available tenders along with tender data.
   a. The bidder then looks for a suitable tender to bid on.
   b. The tender specifications, as well as the tendering organization's contact information, are delivered to the bidder.
3. After that, the bidder submits a bid on the tender by submitting a quote with quotation clauses. The bids are encrypted twice:
   a. once with the bidder's symmetric key and then again with the tender's public key (address of tender on the block chain).
   b. The bidder can only bid during the bidding period, and no additional bids will be accepted once the deadline has passed.
4. Once the deadline is passed the bids are open to the tendering organization for evaluation.
   a. The tendering organization gets the details of all the bids and decrypts the bid using the key provided by the bidder.
   b. Then the bid is evaluated and the credibility and capability of the bidding

ISSN: 2583-3286(Online)

company are checked using the documents provided in the bid. The tendering organization can approve or reject the bid

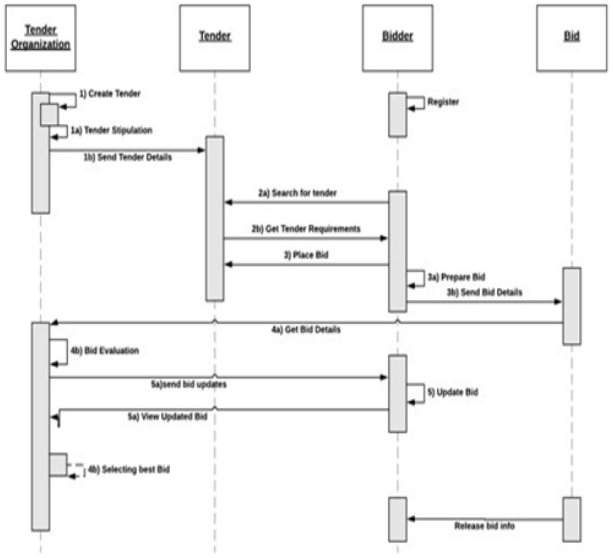

Figure 2. System Design for Placing Bid

The lowest and best bid is then chosen as the winner by the tendering organisation. All bidders are given access to all bidding and negotiation information. As a result, transparency is ensured.

V. METHODOLOGY

As mentioned in the introduction, the implementation details are divided into four sections. The information is specific to the Solidity programming language, which is used to create smart contracts that run on the Ethereumblock chain.

A) Tender Creation and Publishing

Algorithm: creating the tender

ProcedurecreateTender(_tenderTitle,_bidO,_bidC,_description,_address)

tdr ← new Tender()
tdr.manager ← _address
tdr.title ← _tenderTitle
tdr.description ← _description
tdr.bid_open ← _bidO
tdr.bid_close ← _bidC

B) Bidding on tender

Algorithm: Placing a Bid

procedu**r**eBid(_address,_quote,_quoteClause,_documents)

companyAdd ← _address
quoteAmount ← _quote
bidStatus ← "pending"

The bid is first validated for four conditions before it is placed:

- It is checked whether the bid is placed after the bid opening date.
- It is checked whether the bid is placed before the bid closing date.
-
- It is checked whether the tender is not complete.
- It is checked whether the bidder has already placed the bid once.

If any of these conditions are violated, the bid is rejected or else the bid is created using the details provided including company documents.

C) Bid Evaluation

Algorithm: Bid Evaluation approveBid(index)
bids[index].bidStatus ← "approved"
procedurerejectBid(index)
bids[index].bidStatus ← "rejected"

D) Winner Selection and Publishing Bids to Bidders

This function is restricted to the manager who is the one that created the tender smart contract on the block chain. It will publish the details with the winning contractor.

Create a Wallet at Meta Mask

MetaMask is a cryptocurrency wallet that uses software to interface with the Ethereum network. It gives users access to their Ethereum wallet via a browser extension or mobile app, which they can then use to connect with decentralized apps. ConsenSys Software Inc., a block chain software business focused on Ethereum-based tools and infrastructure, created Meta Mask.

Steps to use metamask wallet:-

- Click on Install MetaMask as a Google Chrome extension.
- Click Add to Chrome.
- Click Add Extension.
- Create an account.
- Click on the extension icon in the upper right corner to open MetaMask.
- To install the latest version and be up to date, click Try it now.
- Click Continue.
- You will be prompted to create a new password.
- Click Create.
- Proceed by clicking Next and accept the Terms of Use.

- Click Reveal Secret Words.

Here is a 12 word seed phrase. This is really important and usually not a good idea to store digitally, so take time and write it down. Verify secret phrase by selecting the previously generated phrase in order.

Select a Test Network (using Ethereum (Rinkeby) Testnet network for this).

ISSN: 2583-3286(Online)

In the upper left corner, click “Main Network” Then select “Rinkeby Test Network” The Rinkeby Test Network is used to test the code and get free Ether to test Smart Contracts.

Use Editor Remix to Write the Smart Contract in Solidity

The Remix editor recompiles the code each time the current file is changed or another file is selected. It also provides syntax highlighting mapped to solidity keywords.

Clicking the Solidity icon in the icon panel brings you to the Solidity Compiler. Compiling is triggered when you click the compile button (F. in image below). If you want the file to be compiled each time the file is saved or when another file is selected - check the auto compile checkbox.

Select an Ethereum fork

The “fork selection” dropdown list (in image below) allows to compile code against a specific ethereum hard fork. The compiler default corresponds to the default hard fork used by a specific version. To see the name of the hard fork used in the current compilation, click the “Compilation Details” button(H. in image below) and in the Metadata section will be a sub-section called settings. Open up the settings to see the hard fork’s name.

Deployment of contract

The Deploy the smart contract at the Ethereum test network by Pressing the deploy button at the Remix window’s right-hand side. Wait until the transaction is complete. After the transaction commits successfully, the address of the smart contract would be visible at the right-hand side of the remix window. At first, all the ERC20 tokens will be stored in the wallet of a user who is deploying the smart contract. To check the tokens in your wallet, go to the meta mask window, click add tokens, enter the smart contract address and click ok. You would be able to see the number of tokens there.

VI. CONCLUSION

The main aim of this paper is to remove middle man from the regular contracts and make people aware to use smart contracts bases on ethereum. A detailed description has given to how to make smart contracts in section III. smart contracts are expected to revolutionize many traditional industries, such as financial, healthcare, energy, etc. In this paper, a comprehensive survey of block chain-enabled smart contracts from both technical and usage points of view has been presented. In this paper, about the use of smart contracts implemented in railway tender system has been discussed by using block chain technology, Solidity and Ethereum. With the help of this online tendering system transparency and corruption free system in filling of tenders can be develop. Traditional technology and design patterns cannot be used in applications like tender portals where transparency and security are paramount since they jeopardize these objectives. As previously stated, there are numerous security needs for a tendering framework that cannot be met solely by employing a centralized tender platform to create and bid on contracts. The security and openness needs of this type of application can only be met by adopting fair, open, and decentralized technologies like Block chain and Smart Contracts. This paper discusses how such a system may be constructed by mentioning numerous processes and their fundamental implementation as well as the needs of the tender smart contract.

A detailed overview of various technologies used in making smart contracts has given. Smart contracts methodology are discussed for how to make smart contracts using solidity.

When it comes to applications like tender management, where security and transparency are critical, traditional technology and design patterns can't be employed since they risk data manipulation. There are numerous security needs for a tendering system that cannot be met simply by establishing and bidding contracts utilizing a centralized database or instead of that it is better to use the decentralized database which is block chain.

REFERENCES

[1] V. Buterin, “A next-generation smart contract and decentralized application platform.," Available online at: https://github.com/ethereum/wiki/wiki/White-Paper/ [Accessed 19/02/2017]..

[2] J. Stark, “Making sense of block chain smart contracts," Available online at: http://www.coindesk.com/making-sense-smart-contracts/ [Ac-cessed 06/03/2017]..

[3] Ware,Miss.Sangya . , Rakesh,Mrs.Shanu. K., &Choudhary,Mr.Bharat . (2020). Heart Attack Prediction by Using Machine Learning Techniques. International Journal of Recent Technology and Engineering, 8(5), 1577-1580.

[4] A. Lewis, ”A gentle introduction to smart contracts," Available online at: https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/ [Accessed 25/02/2017].

[5] G. Wood, “Ethereum: A secure decentralisedgeneralised transaction ledger," Ethereum Project Yellow Paper, 2014.

[6] G. Bigi, A. Bracciali, G. Meacci, and E. Tuosto, “Validation of decentralised smart contracts through game theory and formal methods," in Programming Languages with Applications to Biology and Security, pp. 142-161, Springer, 2015

[7] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, “Block chain contract: Securing a block chain applied to smart contracts," in 2016 IEEE International Conference on Consumer Electronics (ICCE), pp. 467-468, IEEE, 2016.