Decentralized E-bidding Governance Application using Blockchain

M.Nikhil Babu

Student, Department of CSE, Baba Institute of technology and sciences,

Visakhapatnam

K S N Murthy

Assistant Professor,Department of CSE, Baba Institute of technology and sciences,

Visakhapatnam, Andhra Pradesh, 530048

Email: ksnm1925@bitsvizag.com

K. Gajalakshmi

Student, Department of CSE, Baba Institute of technology and sciences,

Visakhapatnam

T. Sai Krishna

Student, Department of CSE, Baba Institute of technology and sciences,

Visakhapatnam

P. UshaKiran

Student, Department of CSE, Baba Institute of technology and sciences,

Visakhapatnam

Abstract- Due to technological advancements, traditional paradigms like central databases were challenged. Since society values like mutual understanding and honesty shifted, which implies the expectations of the government also transfers from traditional models to something new technologies which overcome those challenges. Some technologies such as internet play a crucial role on data and the activities between the users and government.

To enable integrity, non-repudiation, evidential along with immutability to the data requires the desirable technology to support the above the requirements. BLOCKCHAIN is a technology which is mainly used to facilitate crypto currencies as a record of transactions. A known example is Bitcoin, recent years BlockChain utility is being recognized through smart contracts. In this paper we propose a concept of smart contract on government tendering scheme. This scheme is implementing in Ethereum platform.

Keywords: BlockChain, immutability, Smart Contract, Ethereum.

1. INTRODUCTION

In this process we have e-bidding initiatives by the use of technology for government activities, fostering transparency, participation and communication for both ends. An association of E- government and open functionalities, supported by new technologies like blockchain has the potential to provide integrity and immutability. By enabling this technology we can provide the information and there is a chance for allowing the users to trace the procedures of the government applications without any unnecessary hassle.

Therefore there is a procedure for exploring the tendering process.

a) Notification for opening a tender.
b) Time period for getting bidding application.
c) Completion of bidding.
d) Choose the best bid.

Main Objectives:

1. The tendering organization can open a tender; once the tender is open they cannot change it. Main objective is to prevent the organisation for varying the activity in favour of bidding organisations and also there is a possibility for evaluation mechanism for the best bid.
2. Authorised organisations can place a bid without any chance in terms of compromising or changing the date which can be placed in a secure location by promoting integrity. And also there is a provision that the organisation does not know the other organisation is placed a bid or not.
3. Once the time period for bidding application is closed then only the tendering organisation can open the bids.
4. Based on the bids placed by the bidding organizations, evaluation committee will evaluate the best bid for the given tender.

2. BLOCKCHAIN

Block chain is a decentralized technology. The invention of the blockchain for Bitcoin made it the first digital currency to solve double-spending problem without the need of a trusted authority or central serverBlockchain is in form of a distributed database. A distributed database is a collection of interrelated databases stored in multiple locations. A distributed database is maintained at separate locations where every participating node has a copy of the database. I.e., they need not to trust each other to trust the data stored in the ledger.

3. SMART CONTRACTS

A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation

or performance of an agreement or transaction. It is the simplest form of decentralized automation. Smart contracts are tampered resistant, self-verifying, self-executing code.

4. GENERIC TENDERING PROCESS

The government procurement process depends on individual governments or geographical zones. The Below is the procurement process and is explained below:

1. Tendering organization(i.e. Government department) creates a tender based on requirements they specify terms & conditions of tender, information about acceptable bid & evaluation criteria.
2. The tender is published to the tendering host. Here the host may be a separate government or part of tendering organization.
3. The Bidding organization interested would download the tender specifications.
4. The tender will be reviewed by the bidding organization and prepare to bid.
5. The prepared bid is submitted to the tendering host.
6. Since there is a limited period specified for bidding the tender host will shut down the portal and won't receive any bids after this period and simply reject those bids which are late.
7. Trending organization will evaluate all the submitted bids as per evaluation criteria and the best bid is selected and notified by tendering organization.
8. Citizens are not involved in this process from steps 1-7 however after evaluation they can request the evaluation result to judge whether the evaluation is fair or not. It may cost both time and money to examine such activities.
9. Through this paper we provide a way that provides reliability, immutability and trust to manage whole bidding process and citizens can evaluate the process by just one click through portal.

5. SMART CONTRACT BASED TENDERING PROCESS

1) A trending organization will initiate the tender through smart contract in blockchain the smart contract having two parameters to examine the tenders.They are:
   a) Certified Public Key.
   b) Evaluation Code for bid.
2) Bidding organizations download the tender.
3) Now bidding organizations will review the tenders and prepares a bid proposal.The main bid is encrypted with generated symmetric key. The Symmetric key is encrypted with public key of tendering organization. Next the final result will be divided to two parts. First part is submitted at the time of division and the remaining part will be communicated at the time of tender submission deadline.
4) The submitted bid is signed by the bidders signature key and pushed into smart contracts. This Signature key is verified whether it is authorized bidding company or not.
5) When the submission time expires, the smart contract will stop accepting the bids.
6) The tendering organization decrypts the bids which is placed by the organization.

7) After decryption, the tendering organization evaluates the bids and select the best bid along with bidders key which is pushed into the blockchain.
8) The Result can be accessed by the bidding organization as well as citizens.
   a) The Bidding organizations get the result from the blockchain placed by the tendering organization which was selected as bid.
   b) Citizens have a chance to evaluate the code from the block using evaluation code to verify the tendering evaluation process is fair or not.

5.1 Rules

Providing Security for the data placed by the stakeholders considered to be as the main requirement in the transparent tendering framework. To satisfy this

I. There is no scope for changing the tender which is deployed in blockchain by the tendering organization.
II. Once the deadline is expired there is no chance for placing the bid. There is no possibility to read the bid by tendering organization.
III. One bidding organization cannot change the bids placed by the other organizations and also there is no chance to see the bid of others.
IV. Bidders cannot mount a Denial-of-Service (DOS) attackon their competitors to stop competitors placing a bid onthe blockchain.
V. Blockchain network or miners cannot affect the tendering process.

6. IMPLEMENTATION

We implemented this tendering process using Ethereum Blockchain API. Ethereum platform is offering a well known development frameworks like Truffle, Ganache, MetaMask, Ripple etc., for developing and deploying smart contracts into Blockchain. We used Truffle framework and solidity to write smart contract, Ganache for local test network and MetaMask for connecting web app to local test network. The below are the algorithms which we used in our smart contract implementation.

Algorithm 1: Initializing a Tender

```
1:procedure REQFORTENDER(_length, _pubk, _limit)
2:    biddingEnd ← TimeNow()+_length
3:    limit ← _limit
4:    pubk ← _pubk
```

Tendering organization requests or initiates the tender by placing contract in a blockchain. This contract is created with a length, given in milliseconds. This time is calculated using the Unix Epoch time. Limit is also

given, which is used to control the number of tenders a contractor can place for this auction. The entity that created the auction is also required to pass in a public key that is specific to this request for tender contract.

Algorithm 2: Placing a Bid

```
1: procedure PLACEBID(id,data,msgHadhed,v,r,s)
2:bidValidity ←ValidBid(id,msgHashed,v,r,s)
3:        if bidValiditythen
4:           bidCount[id]+ = 1
5:      bid← newBid(id,data,bidValidity,bidsPlaced,biddingEnd)
6: returnbid
7:procedure VALIDBID(id)
8:        validHash←verify(msgHash,v,r,s)
9:        validTime←timeNow() <biddingEnd
10:       allowedBid←bidcount[id] <limit
11:       return validHashandvalidTime andallowedBid
12:  procedure BID(_id,_data,_validity)
13:         id← _id
14:         data← _data
15:validity← _validity
```

Organizations interested to participate will prepare and place a bid to the smart contract. We implemented this algorithm to minimize the gas cost between each transactions. When a bid is placed, the address is returned to the contractor, this address could be given to the auction creator external to the transaction.

Algorithm 3: Evaluating All Bids

```
1:procedure MAKEREQUEST(_length, _pubk_limit)
2:    listOfBids← ReqBids( )
3:for bids in listOfBids do
4:        validBid←bids.getValidity( )
5:if validbid then
6:            listOfValidBidDataAddresses.add(validBid.getDataAdress( ))
7:  procedure REQBIDS(_length, _pubk_limit)
8:       afterAuction←timeNow( )> biddingEnd
9:       if afterAuction then
10:           return bidsPlaced
```

Once the tender process is completed its time for evaluation. This is a retrieving algorithm. Retrieving the information does not require anytransactions and thus there is no transaction cost. The client application will receive a list of bids and the best bid is selected. This algorithm runs in O(n) time.

7. CONCLUSION

Traditionally, somehow it is difficult to provide transparency and fair-ness in the government projects because of the investment of both finance and time for all stakeholders. With the increase of open governance, public opinion plays a crucial role in promoting the governance application. To develop that environment blockchain and smart contracts shows great potential. in this paper, the process of government tendering system is taken as an example and implemented through Ethereum Platform in Blockchain Environment. The main objective is to provide the Integrity, Non-Repudiation and transparency using smart contracts to this end, it was successful.

REFERENCES

[1]. https://arxiv.org/pdf/1805.05844.pdf

[2]. https://www.quora.com/What-is-blockchain-technology-1

[3]. https://en.wikipedia.org/wiki/Blockchain_(database)

[4].https://www.researchgate.net/publication/281038087_Optimistic_Fair-Exchange_with_Anonymity_for_Bitcoin_Users

[5]. https://en.decentral.news/public-procurement-blockchain/

[6]. https://blockchainhub.net/smart-contracts/

[7]. http://www.rics.org/en/knowledge/glossary/blockchain/

[8].https://hackernoon.com/can-blockchain-technology-be-used-to-improve-open-governance-2bddb63561fb

[9]. https://www.quora.com/What-is-the-difference-between-smart-contracts-and-dapps

[10]. https://medium.com/@ICOKite/a-beginners-guide-to-smart-contracts-67cf731a7da5