Permissioned blockchain based public procurement system

J J Deshpande, M Gowda, M Dixit, M S Khubbar, B S Jayasri and S Lokesh

Department of Computer Science and Engineering, The National Institute of Engineering, Mysore, Karnataka, 570008, India

E-mail: monisha9gowda@gmail.com

Abstract. Hundreds of public procurement projects are undertaken every day all over the country. The tenders for these projects are given to the winning contractor in an auction-like setting which have massive security issues. After a contractor wins a tender, the specifics of the progress of the work done are rarely properly monitored. The details of the finances spent on the project can be easily manipulated. To enable integrity, non-repudiation and immutability to the data requires the desirable technology to support the above requirements. Hence, the proposed system uses blockchain technology to provide transparency and trust to all parties involved in the network. The entire system consists of two modules such as the Tender Bidding system and Tender Monitoring system using a multi-organization blockchain network in the Hyperledger Fabric. The whole bidding process is improved by creating a decentralized descending auction system that will carry it out fairly and transparently. The Tender Monitoring system employs a custom endorsement policy to attain 100% consensus for attesting every transaction made regarding the progress of the project so that vital steps are ratified and recorded with evidence supporting their integrity. The main aspects of the system, its many components, deployment and drawbacks are viewed.

1. Introduction
The public procurement systems used in various parts of the world are either manual or are a very basic online system with various security, administrative and other threats. An efficient public procurement system improves public administration by tackling problems like corruption, wastage and dysfunction. This becomes vital for achieving the country's economic, social and fiscal commitments. Even though it's importance is recognised, there is still a variety of flaws and the system suffers from incompetence. These systems do very little to prevent corruption and it is easy for individuals to find ways to exploit them. Hence, the future of such systems needs to be secure, transparent, immutable, resilient and fast processing. The system proposed in this paper takes into account the many drawbacks of existing systems and creates a fair and transparent tender auctioning and monitoring environment with the use of the Hyperledger technology. The ideologies that propagated the creation of this system will be looked upon in the next section.

2. Literature Survey
Chen et al. [1] propose a smart contract implemented via Ethereum platform which can ensure the bill’s security, privacy, non-reputability and inalterability owing to all the transactions that are recorded in the same but decentralized ledgers. The system proposed a blockchain technique into the
E-auction to resolve the issue of a centralized intermediary and avoid the bid price leaked by the lead bidder. Hardwick et al. [2] further describes the success of open government initiatives in utilizing technologies that enable access to both the data and to engagement activities between citizens and government. It is observed that the system employs the concept of three smart contracts to government tendering activities enabling a fair, transparent and independently verifiable (auditable) government tendering scheme.

Fukui et al. [3] uses a novel way of public procurement, where the contractor is selected on a multi-attribute basis of quality, price, completion time, technical merit, aesthetic and functional characteristics, environmental characteristics, running costs, cost-effectiveness, etc. The system considers the case in which the government aims to achieve socially efficient levels of quality that maximize social surplus and simultaneously improve the expected utility for the government through competitive bidding. Jain [4] proposes a decentralized system of storing documents using a novel technology, Blockchain. The second tier database will be implemented on a Blockchain fabric, having assets (individual data entries) accessible only via a public and private key pair.

3. Existing System
The system for tender procurement in India [5], [6] consists of five different phases, each explained below.

3.1. Planning of bids
Planning of bids is the stage wherein the documents related to the bid are prepared. This is done by first assessing the entities required for that particular tender and researching the internal and financial needs for the same. Once all these aspects are known, sanctions are issued, costs are laid out and officials are assigned to the tender. A procuring entity is selected for the bid.

3.2. Preparation and Publication of bids
The documents contain the bid fee, earnest money deposit (EMD) or bid security, performance security, etc. information. The EMD of unsuccessful bids must be returned within a given period, although there exists a certain amount of delay for this. Bid documents contain information about the period during which they can be accessed, pre-bid meetings can be held, bid submissions, bid reviews and evaluations. The prepared bids are pushed through e-portals with a reasonable time to access and submit them.

3.3. Submission of Bids and Evaluation
Whence, the decision of submission is taken by the bidder, he/she needs to adhere to the bid timeline and the bid specifications. All the officials and bidders access the portal for the bid using digital signature certificates to validate themselves. The bidders have a specified amount of time to withdraw or modify their submitted bids. The bids must be evaluated immediately but often there is a delay at this stage. The time of evaluation of a particular bid is sent to the bidder and only those bids that qualify are sent for technical evaluation by the officials. After the technical evaluation, the selected bids are financially evaluated.

3.4. Award & Execution
In this phase, the selected bidder is awarded the contract for the bid. The criteria for selection is usually the lowest bidder but since 2017 a newer approach is observed wherein the quality-price criteria is used to select the winning bid. To make this process transparent, the awarding of the contract of the bid is posted publicly and the unsuccessful bidders can also ask for feedback to learn for future bids. The awardee is sent the contract and asked to sign it to proceed with the project.
3.5. Redressal Mechanism
This phase is necessary for a transparent and accountable procurement system. India practices an informal two-tier system where in the first tier, the discontented bidder can take up their concerns to the officials in-charge. In the second tier, the discontented bidder can take their concerns to the court. If the bidder is found guilty in court, the bidder is debarred or banned from participating in public procurement.

4. Problem Statement
Consistent implementation of rules and regulations and an efficient implementation of public procurement help in achieving the desired goals from the country's fiscal outlays. However, these processes are vastly different from the ideal scenario. Issues like a bare bones, sometimes non-existent monitoring process, lack of proper governance and accountability, minimal awareness and much more, plague the already poorly implemented system. Some of the major challenges are mentioned below[5].

1. The absence of a comprehensive procurement Act
2. Lack of standard bid documents
3. Delays in activities in the procurement cycle
4. Unfair practices and corruption
5. Presence of anti-competitive elements create hurdles for the procurement process by negating the best value of money
6. Lack of an independent mechanism to address grievances and complaints
7. Lack of competent and skilled procurement officials

Innovative solutions powered by blockchain technology can help solve this issue with an interactive, distributed, permissioned, multi-organisation network. The whole bidding process can be improved by creating a decentralized descending auction system on a permissioned blockchain framework. The winning contractor starts the tender project. Further, the relevant bills proposed by the contractor can be easily tracked using an immutable decentralized ledger and manipulation of related documents can subside substantially. Each document proposed can be validated by a set of certified official endorsers. The tender project becomes validated only if all the submitted documents are valid.

5. Proposed System

![Multi-Organization Blockchain Network](image-url)

Figure 1. Multi-Organization Blockchain Network.
Hyperledger Fabric based multi-organization blockchain network is constructed of several different elements, the most prominent of which are organizations with everything else built around them.

1. The organizations each own several peers that are essential elements in the network which host the shared ledgers and the chaincode.
2. To conduct private and confidential transactions of a certain set of organizations involved in a particular project, a single common channel is created to connect all of them.
3. A separate Hyperledger Fabric Certificate Authority (CA) is used for each organisation to issue PKI-based certificates to network member organizations and their users.
4. The Membership Service Provider (MSP) component of the system is used to map credentials of the clients and peers for them to participate in the network.
5. The orderer receives transactions from all the endorsing nodes, orders them into blocks and finally distributes them to peers for further validation and commit to the ledger.

In figure 1, a representation of a multi-organisation blockchain business network on Hyperledger Fabric using Hyperledger Composer with four organizations connected to a single Channel 1 is shown. Each organisation owns several peers of which few are connected to Channel 1 while others are usually joined to at least one other channel. Participants and clients access the network through applications.

Applications wanting to update the ledger undergo a series of steps, at the end of which consistency is maintained in all ledgers of the channel.

1. The client calls the blockchain through the application which triggers the transaction proposal.
2. The chaincode is executed on every permission node called the endorsement peer. The result of the execution generates a read-write set called the transaction proposal response signed by ever endorsing peer. This change however, is not reflected in the ledger.
3. The responses from each endorsing peer are collected and compared to reach a consensus based on the endorsement policy.
4. If consensus is reached, the client sends the responses to the orderer. In the case where consensus is not reached the transaction is still forwarded but marked invalid in the ledger by the peer.
5. The orderer (Eg. Kafka) batches all the transactions into blocks and forwards them to every committing peer on the channel.
6. Each peer validates all the transactions within a block to ensure that all relevant organisations have consistently endorsed them. This is done before any block is committed to the ledger and updated in the world state database.
7. All valid or invalid transactions are appended to the blockchain history. However, it's only the valid transactions that make an update.
8. Failed transactions are retained for audit.

The entire proposed system is divided into two modules, each of which is executed on a separate multi-organisation blockchain network. They are Tender Bidding Network and Tender Monitoring Network.

5.1. Tender Bidding on Multi-Organisation Network

To explain the steps taken during the bidding process, a generic framework is used and shown in figure 2. This process is shown and elaborated below.
Figure 2. Sequence Diagram of Tender Bidding Framework.

- The Auctioneer adds the various Tenders’ details to the list of assets.
- The Auctioneer creates the TenderListing with the details of the Tender belonging to the respective government department.
- The Members(Contractors) submit their respective Bid prices in a Sealed bid manner through the Offer transaction for the respective Tender.
- Each Contractor can offer only one final bid per Tender.
- After the allotted time for Tender Bid submissions completes, the Auctioneer submits a Close_Bidding transaction to end the Tender bidding.
- The ownership of the Tender is transferred to the Member(Contractor) whose bid value met the proposed rules and conditions for winning the tender as described in the script.

5.2. Tender Monitoring on Multi-Organisation Network
To explain the steps taken during the monitoring process, a generic framework is used and shown in figure 3. This process is shown and elaborated below.

Figure 3. Sequence Diagram of Tender Monitoring Framework.
• The Contracting Company begins the project it won in the previous bidding phase.
• The company proposes a transaction for every update made in the project (Eg. Documents for Acquiring Materials)
• We implement a custom endorsement policy which requires 100% consensus, i.e all endorsers (Eg: Engineer, Supplier, Labour Representative etc) endorse every update or transaction made into the project ledger.
• If any endorser rejects the document presented by the contractor, the contractor is notified of the invalidity and the transaction becomes invalid.
• The project comes to an end only after all the submitted documents are attested by every endorsing peer. The contractor closes the contract.
• The state of the contract is then made VALID and CLOSED.
• The respective public procuring department which issued the contract, easily analyses all bill documents by tracking the blockchain ledger of the project.
• The government releases the funds to the contractor as per the expense documents submitted.

6. Implementation
In the implementation of the Tender Bidding and Monitoring framework, tools, frameworks and libraries of the Hyperledger Fabric project are used.

Thus, two multi-organisation blockchain networks are created, one for i) Executing the auction for the released tender, and the other for ii) Monitoring the progress of the project issued by the tender.

A number of blockchain systems allow unknown entities into the network with proof of work protocols to validate transactions and secure the network to create an open permission-less system. However, Hyperledger Fabric provides a private and permissioned system where entities enroll with the help of a trusted Membership Service Provider (MSP). It also customizes endorsement policies where trusted organisations validate transactions, thus modeling the real world scenarios.

Every multi-organisation system leverages Docker images to quickly bootstrap a Hyperledger Fabric network that consists of peers representing different organizations. A custom connection profile is created for each organisation. Business network cards are generated and imported for admins and other participants, at every tier of the network to authenticate addition of new members. Certificates and Keys are generated to sign/verify authentication for entities to communicate and transact.

A custom endorsement policy defines which organisations must endorse the transactions before it can be submitted into the ledger. Raft ordering service is used to order transactions and create blocks. A container is launched to execute a script which connects peers to a channel, deploys a chaincode and executes transactions against it, secured using TLS to encrypt communications. CouchDB is used as the world stage database because fast reads and queries are needed.

6.1. Tender Bidding Network
The bidding chaincode contains the following components:

Participants:
Auctioneer: The Respective Government Department in charge of publishing Tender
Members: Public Procuring Department and Certified Contractors

Assets:
Tender: Details of the Tender
TenderListing: Details of the Tender involved in the auction

Transactions:
Offer: Submit Bid-Price by Contractor
CloseBidding: Completes the Tender Auction

1. After the multi-organisation network is generated and configured, the Bidding chaincode is deployed on the channel and the endorsing peers, which runs in its chaincode container and is
instantiated on the common ledger shared across all organizations. Any contractor can participate as a client using an Application connected to the network.

2. Every contractor or entity organisation joining the network to bid is given an identity card as a participant in the network in the form of certificates (public key) and private keys to represent or sign/verify authentication for participants to perform transactions.

3. The Auctioneer initializes the network with the Tender and Tender Listing as Assets and begins the auction.

4. Every participating contractor submits an Offer/Bid as a transaction to the network for the Auction.

5. After the stipulated time interval for the online auction is over, the tender auction ends. All the offers are collected and run through the smart contract logic to calculate the final winner based on submitted bid’s cost-quality weightage. (Eg: Least Bid submitted)

6. The winning contractor is notified of the event.

6.2. Tender Monitoring Network

The Monitoring chaincode contains the following components.

Participants:

Contractor: The Company constructing the project

Endorsers: Engineer, Public Representative, Labor Representative, Government Procuring Department, Supplier

Assets:

Contract: The tender project won by the previous bidding process. It contains the series of endorsed documents submitted by the contractor. The contract state: OPEN, CLOSED, VALIDATED, NOT VALIDATED

Transactions:

Submit_Document: Contractor submits the bill documents.

EngineerValidate: Endorses the transaction with the Engineer’s Sign.

LabourRepValidate: Endorses the transaction with the Labour Representative’s Sign.

SupplierValidate: Endorses the transaction with the Supplier Representative’s Sign.

CloseContract: Closes the contract

The Monitoring Network is deployed in another separate multi-organisation blockchain network with a custom endorsement policy.

1. After the multi-organisation network is generated and configured, the Monitoring chaincode is deployed on the channel and the endorsing peers, which runs in its chaincode container and is instantiated on the common ledger shared across all organizations.

2. Whenever there is considerable progress in the contracted project, an expense document file is submitted as a transaction proposal to the network. The document should be checked and signed by every endorsing peer. A custom endorsement policy requiring a 100% consensus from all the endorsers to validate a transaction bill document is employed as well.

3. Once the transaction responses are collected from the respective peers, the applications can listen to transaction events and check if their proposal is validated. If validated, the transaction proposal and response can be sent to the ordering node to create blocks. Invalidated/Failed transactions can be audited to understand the reason.

4. The ordering nodes create chronological transaction blocks and forward them to every committing peer.

5. Each peer validates the transactions at its end, and if validated, updates the database with the document and appends to the blockchain ledger.

6. When all the expense documents submitted by the contractor are endorsed, validated and updated to the database, the project is concluded.
7. The respective procuring government department tracks the progress and attested documents in the world state database by querying the blockchain ledger of any peer. Once analyzed, the proper expense of the project is calculated and the funds are released by the government to the contractor.

8. The periodic assessment helps in regular tracking of the project’s progress, speeding up the entire process of auditing the project expenses for quick release of funds to the contractor.

7. Results
The proposed system is executed on separate multi-organisation blockchain networks using Hyperledger Fabric on a local virtual system. To execute a scaled system with persistent networks and databases, the use of IBM Blockchain Platform or other secure Cloud environments is required, which easily customizes the network infrastructure as needed, whether that is the location of the nodes, the CPU and RAM of the hardware, the endorsement policy needed to reach consensus, or adding new organizations and members to the network. The system secures the tender bidding process and provides a consensus system for monitoring the progress of the project with a 100% endorsement policy. Table 1 shows the difference between the existing system and proposed system.

| Table 1. Comparing existing system and proposed system. |
|----------------------------------------------------------|
| **Existing System**                                      | **Proposed System**                                      |
| Single point of vulnerability present in traditional databases | Decentralized databases using the blockchain ledger |
| Project data vulnerable to change                        | Immutable blockchain ledger preserves the authenticity of documents |
| Auction process is not free of unfair practices by either the officials or other external elements. | Automating and decentralizing the auction process frees it from social problems that plague the system |
| Centralized Control and validation of Auction and monitoring | Distributed control and validation preventing favouritism, bid-rigging and collusive bidding |
| Cost and interference of third party auction organisations. | Eliminates cost and interference of third party organisations |
| Lack of proper project monitoring                        | Monitoring progress with proper tracking of project documents in the ledger |
| Single point of validation for documents of the project    | 100% endorsement by multiple official endorsers before submission |
| Slow progress due to slow document validation             | Quick document validation helps move the entire system at a faster pace |
| Lack of proper management of contractor compliance        | Proper contractor compliance with Blockchain allows maintenance of a real-time compliance dashboard, indicating to what degree each of their contractors is compliant with a project’s requirements as deadlines approach |

In a general sense, what a lot of different traditional databases bring to the table individually, blockchain brings collectively with an interactive, distributed & permissioned network.

8. Conclusion and Future Enhancements
The current public procurement system of India has mainly five stages, namely procurement planning, bid preparation and bid publication, bid submission and bid evaluation, award and execution of bids, and redressal mechanism. Our proposed system is made more transparent and secure by implementing a decentralized multi-organisation blockchain network. It eradicates unfair practices and corruption via
a transparent and secure system that exists on a network created over Hyperledger Fabric. It
overcomes the hurdle the problem of bid-rigging and dominance by anti-competitive elements as it
aims to create a transparent and fair auction system. The system can be scaled to include a grading
system to determine the winning contractor based on their previous performances in addition to the
auction process. Blockchain helps by making contractors submit the project updates which are
endorsed by various parties involved before appending the immutable ledger. The project can be
scaled to include a feedback portal for the public outside the blockchain network to voice their
complaints and suggestions. Another enhancement for this system is that its monitoring phase can be
deployed for other businesses to help with their project management. All in all, the system has more
advantages to it than the existing system.

Acknowledgments
It gives us immense pleasure to thank our guide Dr. Jayasri B S, Associate Professor, Department of
Computer Science and Engineering, NIE and co-guide Mr. Lokesh S, Associate Professor, Dept of
Computer Science and Engineering, NIE for their valuable suggestions and guidance during the
process of writing this paper.

References

[1] Chen Y, Chen S and Lin I, Blockchain based smart contract for bidding system, 2018 IEEE Int.
Conf. on Applied System Invention (ICASI), Chiba, 2018, pp. 208-11,
DOI:10.1109/ICASI.2018.8394569
[2] Hardwick F S, Akram R N and Markantonakis K, Fair and transparent blockchain based
tendering framework – A Step Towards Open Governance, 17th IEEE Int. Conf. On Trust,
Security and Privacy in Computing and Communications, 2018
DOI:10.1109/TrustCom/BigDataSE.2018.00185
[3] H. Fukui and K. Kobayashi, Optimal comprehensive tendering models for project
procurement, 2010 IEEE Int. Conf. on Systems, Man and Cybernetics, Istanbul, 2010, pp.
3258-3264, DOI: 10.1109/ICSMC.2010.5642303.
[4] Jain A, Jain A, Chauhan N, Singh V and Thakur N, Seguro digital storage of documents using
blockchain, Int. Research Journal of Engineering and Technology (IRJET) 05,
e-ISSN: 2395-0056, Issue: 04, Apr-2018, p-ISSN:2395-0072
[5] Hazarika B and Jena P R, Public procurement in India: Assessment of institutional mechanism,
challenges, and reforms, No. 204, 31-July-2017,
[6] Manual for procurement of works, 2019, Government of India Ministry of Finance, Department
of Expenditure