Analysis of Block Chain based E-Procurement System – A Novel Approach

Priya N\textsuperscript{1}, Ponnavaikko M\textsuperscript{2}, Rex Aantonny\textsuperscript{3}

\textsuperscript{1}Department of Computer Science Engineering, BIST, BIHER, Chennai, TN India
\textsuperscript{2}Vice Chancellor, AVIT, Chennai, TN India
\textsuperscript{3}Founder & CEO Rex Cyber Solutions PvtLtd, Bangalore, India

\texttt{1}priyabiher@gmail.com, \texttt{2}ponnav@gmail.com, \texttt{3}rex@rexcyber Solutions.com

Corresponding Author: Priya N

https://doi.org/10.26782/jmcms.spl.2019.08.00018

Abstract

In recent years everything is digitalized in the world. E-procurement is one of the services used by the government in business sectors. Security is the main aspect of this e-procurement method. In existing systems, various cryptographic mechanisms are used. Recently blockchain made a tremendous change in business and economic activities. blockchain is a distributed ledger that stores the transactions in a secure and immutable way. In this paper Blockchain mechanism is introduced in the proposed system for a secure E-Procurement system. Hyper ledger composer supporting e-procurement framework is designed. Few consensus algorithms in blockchain are discussed to support the blockchain method.

Keywords: E-Procurement, cryptography, security, block chain, consensus, hyper ledger composer.

I. Introduction

The development of the Internet creates a tremendous change in our regular lifestyle. Nowadays most of our transactions are used to hold in online only. Governments and organizations are providing their services to people through the internet. E-Procurement is one of the main processes which is used to negotiate terms of contracts between the suppliers and buyers in government as well as business organizations. Public sector used this E-Procurement for its efficient working with minimal cost. Also, it provides transparency to their services. This transparency in government activities yields to most efficient and corruption less governance.[I] This e-procurement is implemented in various countries now. Security is the main aspect of the field of an E-Procurement system. Many risks and challenges in that system are removed by introducing blockchain technology.
A blockchain will provide one more layer for the existing security mechanisms of the e-procurement system. The blockchain is a distributed ledger which can save all the transactions between two parties efficient and a verifiable manner. Using blockchain technology the data from the whole digital world are prevented from deletion, tampering, and revision. In the present world, all process, tasks, agreement, payment is recorded digitally. A Blockchain stores all information in a database more securely. It is an Internet database which supports decentralization. It can be applied in the platform which enables multiple authoritative domains, who do not trust each other to collaborate or coordinate in a decision-making process. The main functionalities of Blockchain are reduced cost, increased speed, increased security, reduced fraud, and reduced risk. India can aim to use this blockchain technology in various fields. Our aim is to boost this technology for the development of India.

This paper is framed as follows. Section 2 involves the related works which give the usage of blockchain in E-Procurement. Section 3 explains the basics of the blockchain. Section 4 provides the details of consensus algorithms. Section 5 gives the most recent use cases. Section 6, 7 explains the Hyperledger composer with proposed framework for e-procurement system. Finally in section 8 Conclusion and References.

II. Related Works

A. E-Procurement:

E-procurement has been used in many countries nowadays for developing their businesses. Most of the government agencies and private enterprises prefer this e-procurement because of its transparency and less cost with minimal time nature. The government adopted this e-procurement to yield a good governance system. A lot of countries started to use this e-procurement process already for their businesses.

Blockchain is used by worldwide now. Most of the countries are used to implement the blockchain in their governance activities. Lack of Transparency is the main issue of the traditional procurement system. That issue is removed and make the data transparent to all citizens to avoid corruption while using this e-procurement process. Introducing e-procurement provides transparency, increased efficiency, increased accountability and increased service performance.

B. Security Methods In E-Procurement System:

Most of the transactions in the e-procurement process involve very sensitive data. Security should be maintained not only with a stored data also by transforming the information in all transactions. High level of security should be maintained with proper authentication and access control. The policies used in the e-procurement process should not violate the laws and security policies of the country. Indian IT-act designed a well-defined laws for online submission of documents, electronic records, and digitally signed documents.

In the Indian procurement system, the security is implemented in both storage and transactions by some of the following features like valid digital signature, Using...
Time Stamping services, 128-bit encryption with SSL security, A biometric accessing option and a bid based authorization given to authorized personnel to perform tasks such as tender floating, bidding, opening, etc.

A Lot of security methods are followed by the e-procurement system previously. Yuan Zhang, He Zhang [V] projected a mechanism accustomed realize the attainable cheating methods of the bidders conjointly they supply a theoretical guarantee on the competitive quantitative relation for the resource that is purchased by the customer. Donghyun Min, Donggyu Park [VI] proposed a method called Amoeba to protect from ransomware attacks which causes financial damages to important data. Mostly errors or mistakes in procurement lead to high cost and mismatches with the functionality. Shahriyar Mohammadi, Hediy Jahanshahi projected a brand new design for secure E-tendering system during which Authentication is incredibly correct to avoid non repudiation in contracting systems. In this a combination of the bell-lapadulla security model and Shamir cryptosystem are urged to be used for saving tender documents was projected in 2009.

Rong Du, Colin Boyd, and Ernest Foo in 2009 designed a secure e-tender submission protocol used to prevent submission time dispute. Peng Jiang, Fuchun Guo, Willy Susilo, Xinyi Huang, and Joseph K. Liu [VII] introduced an efficient protocol that encrypts all items without the use of buyers’ public keys and used for universal buyers with reduced cost. Wenbo Shi et al [VIII] established a verifiable sealed-bid multi qualitative-attribute-auction protocol solves the Privacy-preserving multi-qualitative-attribute winner determination problem.

C. Worldwide Application Of Blockchain In Government Activities:

In recent years block chain has been used in many industries because of its decentralized nature. Everybody attracted by this mechanism and trying to apply in various fields. This technology overtakes the existing security mechanisms with lower cost solutions. Kumaresan Mudliar, Harshal Parekh, Dr. Prasenjit Bhavathankar [IX] planned many applications of blockchain system integration it with the national identity of a private. In Republic of India national identity like Aadhar is used in centralized applications. Integration Aadhar with blockchain provides the applications in an exceedingly decentralised, secure and clear manner. Their future scope is combining all identities like passport, aadhar, driving license with blockchain technology and can be used for endless applications. Ahmed Alketbi, Qassim Nasir, Manar Abu Talib [X] mentioned the potential use cases and application of Blockchain to change government services. Blockchain delivers government services during a cheaper, distributed and voluntary manner. Amool Sudhan, Manisha J Nene in Employability of Blockchain Technology in Defence Applications introduced a NEMO (Network Enabled Military Operations) model to represent the parameters and resources concerned in military operations during a networked surroundings. Use of blockchain technology in NEMO guarantees security, accessibility, and integrity of information communicated.

Raghava Rao et al. [XI] found that the employment of blockchain technology will facilitate social business in developing the sure relationship with social investors and sponsors. They know the opportunities that blockchain technology will offer transparency, auditability, privacy and decentralization within the domain of social
business. NourDiallo et al. planned a blockchain technology and decentralized autonomous organization (DAO) for rising the e-government system, that is that the first system allowed period of time observance associate degree sensible analysis of an e-government service. The blockchain-based government DAO definitely solves the issues faced by maintenance in advanced IT infrastructures. Heng Hou discussed using blockchain technology and make government activities more efficient in China. The government of Chancheng started exploitation this blockchain and facilitate the govt. activities for developing a private system in society, not just for voters however conjointly for establishments. Also, it improved the supply of services, governance, and government quality. This blockchain based mostly technology ensures election security and integrity and transparency. Using blockchain in various fields like banking, healthcare, and businesses and in government sector yields a lot of benefits.

D. Blockchain in e-procurement systems

Introducing the blockchain mechanism in e-auction was discussed in [XII] because of its decentralized nature. Yi-Hui Chen used blockchain technology to remove the transaction cost and improve electronic seals confidentiality, non-repudiation, and unchangeability. The smart contract is employed to avoid the unseaworthy of terms by the lead bidder. XU Hao, SHI Xiao-Hong, Loloish Dian planned a multi-agent e-commerce system supported blockchain technology. In this paper author used twin SHA-256 with a RAFT algorithmic rule for verification code in knowledge storage. The hash perform is combined with the RSA encoding algorithmic rule to handle data. By confirming the authentication of the handling data stop tamper safe and reliable commercialism method is achieved.

III. Blockchain Basics

Blockchain was proposed by Satoshi Nakamoto in 2008. The problems like more cost for mediation in the transaction, non-reversible payments, non-reversible services are solved by this block chain method. The blockchain is the most powerful technology which is being initially used for bitcoin then started using in many other fields like finance, real estate, government, sector, music industry, health care systems. Blockchain may be a secure decentralized ledger nothaving a central authority. Blockchain will record the transactions between 2 parties expeditiously during a verifiable and permanent manner. Block may be a linear arrangement that carries all transactions. every block contains a block header and transactions list. each block inherits from the previous block, the hash price of the previous block is employed to form the new block’s hash to create the blockchain tamperproof. The header of the block connects the transactions. If anyone changes the transaction it will show its effect in the block header. The header of the subsequent blocks has framed the chain. The entire blockchain needs to be updated if any changes happened anywhere.
Tampering is a difficult process as the chain grows. In that, it is extremely hard to make the changes. In this BC, a hash function is used to connect the blocks in a tamperproof way. There are two models in the blockchain network, one is permission less, and another one is permission. Permission-less is an open environment that is suitable for financial applications like cryptocurrency. Permission blockchain model is used for business applications like smart contracts.

In the blockchain mechanism[III], the consensus is required to achieve an honest and transparent financial system. In the decentralized distributed ledgers consensus plays an important role among every member to gree on the value of the data inside the ledgers. In all transactions, the consensus is included in the ledger and accepted as a common truth.

IV. Analysis Of Consensus Algorithms

Consensus algorithms are the root of blockchain architecture. Consensus gave the decision making for a group, where the members of the group support the decision that gives the best results for the others. Other members have to agree with the decision whether they like it or not. Consensus algorithms are framed not only the majority supporters but based on the maximum benefits they got. The objectives of consensus are collaboration, cooperation, equal rights, participation, and activity.

The nodes connected in the network must reach an agreement. If a single fault occurs, nodes cannot accept the agreement. Consensus nodes are more reliable and fault tolerant. If any of the nodes starts behaving maliciously (byzantine fault), to rectify that some of the consensus algorithms like Raft, Paxos, Byzantine fault tolerance are needed. For giving the best output or results suitable consensus algorithms are necessary.

Proof-of-Work (PoW) is the first blockchain algorithm. This confirmed the transaction in the network and produce relevant blocks in the network chain. The miners (independent nodes) will solve the cryptographic puzzles based on cryptographic hashes then only new blocks will get created, after that the transactions are confirmed. Depends upon the difficulty in solving the puzzles then the speed of creation of blocks is delayed. This process requires a lot of computational power for solving. More electricity power is needed to maintain hardware. PoW protocol implemented in Bitcoin uses SHA-256 as the hash function. Ethereum is used in PoW for making the smart contracts. Proof-of-Stake (PoS) is energy efficient when compared with PoW. It does not require heavy hardware backup. The concept of PoS is the individual nodes having more cryptocurrency had the authority to validate the transaction and create the block. The main disadvantage of this PoS is that full
decentralization is impossible here. Some of the popular cryptocurrencies using PoS are PIVX, Navcoin, Stratis.[XIV] In PoS the individuals having more coins did the validation. So the system turns into a centralized community. To prevent this Leased Proof-Of-Stake (LPoS) is introduced. Small stakeholders can lease their coins and get benefits.

Proof of Elapsed Time (PoET) is used for permissioned blockchain network. Every individual node has given as a timer object to wait for the random amount of time. The participant who finished his/her share of waiting time will get to be on the ledger to create a new block. Intel proposed new trusted hardware called SGX (Software Guard Extensions). But the problem faced by author is all miners have monetary incentive to energise their mining setups with low-cost and also the SGX enabled hardware is running idle. Finally, the hardware is wasted and this referred to as stale-chips issues. IttayEyal projected associate [XV] an alternate approach or this supported identical trusty hardware infrastructure that has stalechipsdrawbacks. Miners use the SGX only for the useful work and attest that work dedicated to mining that particular block. Also, SGX is manufactured by INTEL, so the consensus model dependent on a third party.

Practical Byzantine Fault Tolerance algorithm (PBFT) designed for asynchronous systems that functions only when the malicious nodes operate on the system. All the nodes reach an agreement based on majority voting. It can finalize the transaction without any confirmation. If any of the nodes agree with the specific block then it gets finalized. The main benefit of PBFT is there is a low power consumption than PoW. The main flaw of this algorithm is the number of nodes increased then the communication between them becomes more complex and the scalability of the system gets reduced. PBFT is more vulnerable to Sybil Attacks.

Simplified Byzantine Fault Tolerance (SBFT) algorithm collects all blocks and group them accordingly into another block and then finally validate all blocks together. Certain rules are followed for validation. Blocks are validated using their own signature. There are several stages like the creation phase, submission phase, and validation phase in this SBFT algorithm. An account manager is used to store all assets securely. For providing more security and privacy three types of techniques are followed such as Zero-knowledge proofs, one-time use addresses, and encrypted metadata.

Delegated Byzantine Fault Tolerance algorithm (DBFT) is more advanced and updated version of PoS consensus systems. NEO uses this DBFT for its transactions. Gas is the execution fee for every operation mode in Ethereum. For more staking, more gas will get by NEO.DBFT designed to focus on better scalability and improved performance. Directed Acyclic Graphs (DAG) is a seamless graph where data gets stored topologically. DAG represents side-chains.[XVI] They allowed different transactions processed independently in the multiple side chains. It blocks less nature so that it can handle the transactions faster.

Combining the features of PoS and PoW a new hybrid is created called Proof of Activity(PoA). It provides more security to any attack and using less power consumption. In this, miners mine the block templates then the system converts into
Proof-of-Stakes. The header information inside the block points to the random stakeholder. These stakeholders then validate the pre-mined blocks. Decred and Espers blockchains adopted the PoA.

Proof-of-Importance blockchain consensus protocol is also the development of Proof of Stake. NEM introduced a new idea called harvesting in PoI. It determines whether a node is eligible to be added to the blockchain or not. The important characteristics of the PoI are vesting, transaction partnership, the scoring system. Proof-of-Capacity (PoC) consensus is the upgraded version of the proof of work. The main characteristics of the PoC are plotting and mining. PoC makes the system faster than Pow. The main drawback is this process creates redundant disk spaces.

Proof of Burn (PoB) consensus protocol is used to protect the cryptocurrency by burning the coins. Here the damage is temporary but the protection will be longlasting. This burning process increases the number of stakes. This consensus protocol is used in the counterparty for protecting cryptocurrency. It produces decentralization distributed network. But burning procedure made a loss in the miners' profit. Proof-of-Weight (PoW) is the upgrade version of the Proof-of-Stake algorithm. Cryptocurrencies like Algorand, Filecoin, and Chia implement the PoW consensus protocol. The Proof-of-Weight owning more tokens like PoS.

A lot of algorithms are helping in blockchain to maintain decentralization nature and transparency. Because of this nature, we make a full stop for the corrupted and faulty systems. The main advantage of these algorithms is we can change them for giving better results.

V. Blockchain-Use Cases

The whole world is slowly transformed into blockchain technology. Bitcoin is the first cryptocurrency which used blockchain. But now a lot of usage of blockchain is found in various fields. There are more than hundreds of use cases in the real world. World economic forum predicted in 2015 15% GDP will be affected by blockchain development. Here we analyzed a blockchain use cases and applications but not sure all will be a successful one. Blockchain use cases are categorized to the impact of the corresponding field. For Protecting government and commercial systems from data theft use of Factom systems gain transparency, honesty, integrity, and security. Essential.one is a data management framework built on top of the blockchain and provides a modular decentralized and Interoperability. GuardTime provides a cybersecurity project that aims to utilize its own Guardtime’s KSI technology primarily designed for enterprise solutions. Remme could also be a cybersecurity blockchain project that improves the present standards of security for every users and companies UN agency are trying to defend their info from unauthorized usage and handle the cyber attacks. In the financial world, PeerNova provides the best-using blockchain in Bigdata and cloud technologies and offers secure and verifiable, retraced data. Barclays bank provides a blockchain based environment to support transparency and integrity.

Aeternity is a smart contract interface that provides transparent governance and provides a new consensus algorithm. Provenance is a blockchain platform that
powers the supply chain and enables businesses to build trust, also provides a transparent environment. SKUChain wants to empower every participant and creating a global value chain. This makes the enterprises to make decisions and bringing better control over the supply chains in an easier method. Estonia, a country in northern Europe, had an e-residency program supported by blockchain by providing ID cards for voting Georgia’s National Agency of Public Registry for land registration. The US state of Delaware created blockchain services for smart contracts. Dubai moved all its official documents secured by blockchain technology by 2020. Samsung SDS partnered with the South Korean government to create a more transparent environment in public safety, welfare, and transportation using blockchain. Meet Democracy Earth is a unique project that aims to build a sovereign democratic government protocol that is open source and builds liquid democracy, data ownership, and borderless governance. Uniquity is the best blockchain use case in the real estate industry. It provides a SaaS application that runs on the top of the blockchain which offers transparency, integrity, and security. Public Registry is one of the unique blockchain applications by which citizens can register their property and store it as a digital asset. It used cryptographic proof and published in Bitcoin-powered blockchain. KASHA is a decentralized social media network that protects user’s freedom of expression by providing privacy, access to information that is built on the top of Ethereum.

VI. Hyperledger Composer

Hyperledger fabric is a blockchain framework used for developing blockchain based products. All transactions in the blockchain network are controlled by the hyperledger fabric. Fabric indicates the certificate authority which issues the certificates for the authorized users. Hyperledger has three types of peers within the given network. Committing peer, Endorsing peer, ordering node. The consensus is achieved by the transaction flow of endorsement, order, and validation. Endorsers proposed the transactions. Ordering service collects all the transactions and delivers to committing peers using different ordering algorithms like SOLO and Kafka. Every committing peer validates all the transactions and provide client applications and updated the final state of the blocks in the blockchain.

Hyperledger composer indicates as an application development framework which made the blockchain applications easier. It allows the participants to send transactions that exchange assets. Here assets mean goods, services, properties all included in the business networks. Assets are a unit having distinctive identifiers. Assets area unit associated with alternative assets or alternative participants. Participants area unit members of the business network. They own the assets and submit the transactions. Every participant having own symbol which has business network cards. These cards alter the method of connecting to a business network with a safer manner.
VII. Basic Framework

Basic framework for blockchain based E-Procurement system connected the participants involved in the process. The steps involved in e-procurement are informing, tendering, auctioning, vendor management, catalogue management, and purchase order integration, order status, ship notice, and invoicing, payment and contract management. All above mentioned are called assets. Each participant placing a bid on an asset in an auction. An auctioneer automatically transferring the assets to the highest bidder and closed the auction. By using queries data can be extracted from the using blockchain network. These queries are sent by using the hyperledger composer. The main goals of hyperledger composer are making the business concepts simple and develop the applications more cheap and quick with less risk and more flexibility.

Creating the tender→publishing the tender→Bid submission→Bid evaluation→Award of contract

In the above procedure of e-procurement systems. Ethereum also used to make the functioning of the smart contract efficiently. Smart contracts stream line the whole process and save time and money.

---

**Fig:2** hyperledger composer

**Fig:3** Comparing the traditional security methods with blockchain technology
VIII. Conclusion

The growth of technology and storage affected the activities of the government and private sectors. Blockchain put a step forward in procurement organizations for further improvements from streamlining the paper-based process. The blockchain is definitely creating a revolution in e-procurement systems. Blockchain applied for transparent business activities with trust and avoiding risks in public sector. In this paper, the study of applying blockchain in e-procurement systems is discussed. It also provided an analysis of different consensus algorithms used in the blockchain. For implementing blockchain, hyperledger composer is chosen. The scope of further research provides fast efficient and optimistic algorithms for blockchain technology. It will help the procurement systems with perfect fraud-free supply chain and made the transactions fast and secure. These studies expecting corruption-free government services.

References

I. Anuradha.C, Khanna.V, “Improving network performance and security in WSN using decentralized hypothesis testing“Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016.

II. Anuradha.C, Khanna.V, “A novel gsm based control for e-devices“Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016

III. Kavitha, R., Nedunchelian, R., “Domain-specific Search engine optimization using healthcare ontology and a neural network backpropagation approach”, 2017, Research Journal of Biotechnology, Special Issue 2:157-166

IV. Kavitha, G., Kavitha, R., “An analysis to improve throughput of high-power hubs in mobile ad hoc network” , 2016, Journal of Chemical and Pharmaceutical Sciences, Vol-9, Issue-2: 361-363

V. Kavitha, G., Kavitha, R., “Dipping interference to supplement throughput in MANET”, 2016, Journal of Chemical and Pharmaceutical Sciences, Vol-9, Issue-2: 357-360

VI. Pothumani, S., Sriram, M., Sridhar, J., Arul Selvan, G., “Secure mobile agents communication on intranet, Journal of Chemical and Pharmaceutical Sciences”, volume 9, Issue 3, Pg No S32-S35, 2016

VII. Pothumani, S., Sriram, M., Sridhar , “Various schemes for database encryption-a survey”, Journal of Chemical and Pharmaceutical Sciences, volume 9, Issue 3, Pg NoS103-S106, 2016
VIII. Priya, N., Sridhar, J., Sriram, M. “Vehicular cloud computing security issues and solutions” Journal of Chemical and Pharmaceutical Sciences (JCPS) Volume 9 Issue 2, April - June 2016

IX. Priya, N., Sridhar, J., Sriram, M. “Mobile large data storage security in cloud computing environment-a new approach” JCPS Volume 9 Issue 2. April - June 2016

X. P. Zahradnik, "Equiripple Approximation of Low-pass FIR Filters Equiripple Approximation of Low-pass FIR Filters", IEEE Transactions on Circuits and Systems II: Express Briefs, Issue: 99, pp. 1-5, 2017

XI. P. Zhao, J. McNeely, P. Golconda, M. A. Bayoumi, R. A. Barcenas, W. Kuang, "Low-Power Clock Branch Sharing Double-Edge Triggered Flip-Flop", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol.: 15, Issue: 3, pp: 338 - 345, 2007

XII. R. Kubasek, Z. Smekal, E. Gescheidtova, K. Bartusek, "Design of Two-channel Half-band Bank of Digital Filters using Optimization Methods", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, page: 151, 2006

XIII. S. Archana, G. Durga, "Design of low power and high speed ripple carry adder", International Conference on Communication and Signal processing, pp: 939 - 943, 2014

XIV. S. K. Mitra and J. F. Kaiser, Handbook for Digital Signal Processing. New York, NY, USA: Wiley, 1993.

XV. S. Samadi, A. Nishihara, H. Iwakura, "Universal maximally flat low pass FIR systems", IEEE Transactions on Signal Processing Vol: 48, Issue: 7, pp: 1956 - 1964, 2000

XVI. Wen Bin Ye, Xin Lou, Ya Jun Yu, "Design of Low-Power Multiplierless Linear-Phase FIR Filters", IEEE Access, Volume: 5, pp: 23466 - 23472, 2017

XVII. X. Zhang, K. Intosume, and T. Yoshikawa, “Design of low delay FIR half-band filters with arbitrary flatness and its application to filter banks,” Electron. Comm. Jpn 3, vol. 8, no. 10, pp. 1–9, 2000