Application of Blockchain Based e-Procurement Solution for Mitigating Corruption in Smart Cities Using Digital Identities

Arish Siddiqui[1], Kazi Tansen[1] and Hassan Abdalla[1]

[1] University of East London, Docklands, London, UK
a.siddiqui@uel.ac.uk ; k.tansen@uel.ac.uk ; h.abdalla@uel.ac.uk

Abstract. Procurement is an important governance tool that is used by the government and development agencies globally to manage and fulfil their complex development plans. However, corruption is a persistent and pervasive issue that hinders ethical progress and it can have a detrimental effect on the outcome of the proposed project that involves more than a few stakeholders. The implementation of Blockchain based e-procurement has been suggested as the potential solution due to its underlying characteristics of immutability and disintermediation. Blockchain technology utilizes distributed consensus, offering evident advantages to procurement by using the digital identities of the stakeholders in the bidding process and maintaining the privacy and security of the contract. This paper systematically maps and implements the existing literature to comprehend the utilization of Blockchain technology in the procurement domain and its potential to mitigate corruption in tender-based environments in smart cities by using digital identities.

Keywords: Blockchain, Digital Identities, Procurement, Smart Cities, Smart Contracts

1. Introduction

Corruption in the procurement process has made countless international headlines in recent years. Due to its complexity and length, the traditional procurement route exhibits a lack of transparency that exposes the potential for corruption. The processes and actions involved in procuring supplies, services, or items from any external supplier or source are referred to as procurement [1]. The procurement process is considered to be a challenging organizational process that involves several functional areas or divisions. Moreover, for effective administration of the entire process, significant amounts of organizational resources are often required. Tenders are habitually prone to the possibility of corruption because of the convoluted nature of the traditional procurement procedure. Contiguous alliances between public sector representatives and outside sources or commercial groups exacerbate the susceptibility to corruption in public procurement, suggests a report released by the Organization for Economic Co-operation and Development [2]. The study established that corruption in the procurement process is the second-most prevalent kind of economic crime to be reported globally. According to an analysis by Transparency International, corruption in public procurement has the regrettable ability to aggrandize the cost of any public project by

50%, which in turn plunges the quality of the product [3]. Many organizations worldwide have implemented a variety of techniques over the years to establish transparency and mitigate corruption in both public and private areas of procurement. However, because of the centralized and intricate nature of the procurement process, corruption in the industry is still very much an obstacle. Blockchain is drawing a lot of attention from researchers due to the transparency, immutability, convenience and reliability of this technology. The decentralized construction of this technology endows a distributed consensus where data is immutable and transactions are verifiable. As a result, the benefits of transparency, efficiency, security, flexibility, cost-effectiveness, and many more may be flawlessly attained with the precise application of Blockchain. This paper confers Blockchain technology with an emphasis on its accessibility and expediency in consort with proposing a Blockchain-based approach incorporating Digital Identity to mitigate corruption in the procurement procedure.

2. Research Methodology

The authors decided to combine the qualitative and non-experimental research methods in order to perform the study. It is typical practice in the research sector to collect and analyze data using qualitative research to understand pertinent ideas [4]. In qualitative research, relevant entities are examined in their natural environments when data may not be available in numerical form. This method is empirical and is physiognomically focused on seeking the answer through "why" and "how" based examination [5]. Qualitative research allows for the adaptability of data gathering and investigation as new ideas emerge. This method allows for the exhuming of unique issues since data collection takes place in realistic settings. Besides, a secondary research technique was adopted to carry out the qualitative research study. Since this procedure is intended to synthesize previous findings for methodical examination, it provides those conducting the studies with the opportunity to appreciate the work already done in the relevant sphere and develop embryonic investigational maneuvers by using the information. The use of secondary research facilitates insight to be attained by carefully examining earlier or existing research, which is important for conducting a unique study. This research approach can be advantageous in achieving the project's goals since it is indispensable to apprehend the scope of Blockchain technology to address the concerns with corruption, transparency and security in the procurement itinerary. Contrarily, non-experimental research allows researchers to appraise factors that occur spontaneously without external interference. This approach can be utilized when the study area is extensive and exploratory, and when there is inadequate information readily available regarding the pertinent research field [6]. In this approach, non-experimental research has the ability to quantify and designate how closely related the variables are to one another. It is imperative to mention that the two main categories of non-experimental research methods are correlational research and observational research. The statistical link that exists between variables but cannot be altered is what drives correlational study. During the implementation of the observational research method, researchers perceive how the contributors behave without obtruding with the variable. In the perception of the project's goals, observational research methods can be utilized since the potential of Blockchain to address the issues is a reliable variable while Corruption or issues with transparency that arise during the

procurement process are independent variables and none of the variables are subject to researcher manipulation.

3. Procurement Process

Procurement refers to an organizational procedure that involves the acquisition of products, materials or services from an outside source [7]. The services or goods that are typically acquired include but are not limited to, office supplies, fixtures, technical apparatus, raw materials, training, testing, recruiting etc. Any public organization is required to prioritize procurement because any services or products obtained through it are accounted for with money from taxpayers [8]. A trustworthy and open procurement process is indispensable to protecting the public interest and ensuring that services are provided to a high quality. The research from the Organization for Economic Co-operation and Development states that the public procurement process is the most predisposed to corrupt practices [2]. The probability of corruption is further intensified by the adjacent coalition between officials from government bodies and commercial entities. The study also highlighted that governmental procurements accounted for almost 4.2 trillion euros in expenditure in OECD nations. Evidence from a number of sources specifies that above 50% of testified incidents of foreign bribery were associated with public organizational procurements from a variety of industries including construction, transportation, information and communication technology, and so on according to foreign bribery report [9]. The likelihood of subsidiary overheads like declined foreign investment and inadequate market access upsurges when there is corruption in public procurement. According to a Transparency International report, the process of procurement is fragmented into the following four key phases that introduce diverse opportunities for corruption, including bribery, deceitful tender obedience, embezzlement, bid rigging, administrative influence on bid assessment, and misuse of power [10].

Fig. 1. Public procurement phases

A general framework may be built to comprehend the functionality even if the public procurement procedure relies on the unique government [11]. According to the requirements, a government agency normally circulates the tender description and starts the procurement procedure. The following phase is for potential participants to evaluate the specifications and submit a tender. After evaluating the submitted bids in line with the requirements set forth, the government organization decides upon the preeminent proposal. However, inadequate transparency and bureaucratic intricacy are fostering a culture of corruption in public procurement, which diminishes citizens' expectations of their government, deters foreign investment, and eventually impairs the economy [11]. As an illustration, one of the prevalent construction establishments in Latin America, ‘Odebrecht’, was convicted of disbursing bribes totaling almost

$800 million in exchange for being awarded different public sector contracts and projects [12]. The Brazil-based engineering establishment filed for liquidation as a result of the public corruption probe. However, the preponderance of Odebrecht's debt, which had been retained by the state bank, eventually resulted in a $25.3 billion liability for Brazilian taxpayers. By creating an impartial, safe, decentralized, and trustworthy procurement architecture that is able to accomplish the entire process transparently, a corruption-free procurement system is feasible [13]. Blockchain technology has been proposed in numerous research to establish an impartial, secure, trustworthy, and transparent public procurement system where all the information, such as competitive data and tender quotation can be handled without being susceptible to exploitation or data counterplots. By facilitating a decentralized defense mechanism, Blockchain technology conserves data integrity and quality [14].

4. Blockchain

Blockchain is a type of distributed ledger that stores transaction data in units called ‘Blocks’. The block that contains a link to the preceding block stores a collection of transactions. A chain of blocks in chronological sequence is created as a result [14]. The principal component of Blockchain is a distributed ledger, via which data may be added to and reformed utilizing the network's consensus process between nodes. A replica of all the records in a sequence of interconnected systems is stored on each liaising node in a Blockchain where transactions are traceable, transparent, and tamper-proof since it incorporates the utilization of a P2P network, distributed consensus, pseudonymity and cryptographic mechanisms [15]. The following figure exhibits a simplified Blockchain structure.

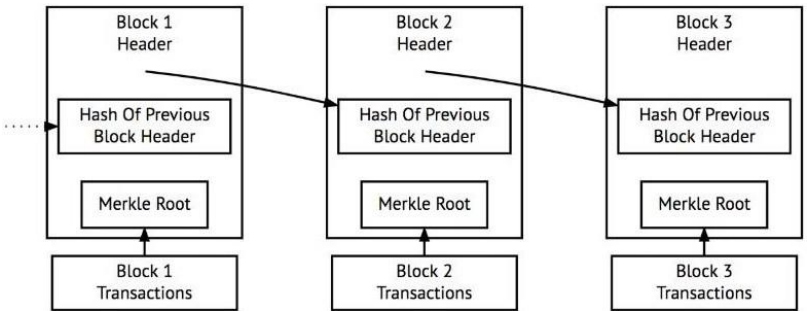

Fig. 2. Simplified Structure of Blockchain [16]

A cryptographic hash function is utilized in a Blockchain to connect consecutive blocks in such a manner that any update to the transaction data in Block 1 would modify the hash value of Block 2, which would subsequently change the hash of Block 3. In the case that the block is even slightly altered, this approach produces a readily apparent disparity [17]. Due to the enormous popularity of cryptocurrencies, Blockchain has generated a lot of interest in recent years. The idea that Blockchain is solely used for cryptocurrency is arguably the largest misperception about it [18]. As a Distributed Ledger Technology, Blockchain primarily emphasizes offering a set of

protocols and procedures for the dissemination of records across several nodes in a cooperating system. The following are fundamental properties of Blockchain technology.

- **Decentralisation:** The process that makes it possible to distribute and constrain control from a centralised authority or place is known as decentralisation. Without the requirement for a reliable third party, decentralisation has the aptitude to enable transparent data exchange. The architecture of decentralised system assurances that information is maintained by all entities rather than being stored by a single one [19]. Blockchain enables resilience from a single point of failure problem since transactions are stored as blocks in a distributed P2P network [20]. Decentralisation surpasses the trust issue by empowering various nodes to administer the network.

- **Transparency:** A dynamic record of every transaction that has already taken place is available on the Blockchain, which is a distributed ledger. There are five commonly identified indispensable qualities for the foundation of transparency [21]. These are accessibility, instructiveness, usability, auditability and comprehensibility. By enabling encrypted access to the data, accessibility is provided in the Blockchain network. To validate the transaction in nodes at various networks, the processing power of Blockchain supports the aptitude of operation and performance in terms of usability. Blockchain offers permanent storage of comprehensive information in the form of blocks, where each effort at modification results in the formation of a new block that comprises a reference to the original data of the preceding block. This endorses instructiveness. By encompassing pertinent data about transactions and smart contracts, including indispensable information for forthcoming authentication in blocks, the Blockchain delivers comprehensibility. Through an algorithm that substantiates the settings and prerequisites prior to accruing new blocks, Blockchain technology guarantees auditability.

- **Immutability:** Immutability in the context of Blockchain technology refers to its ability to be unaltered and irrevocable. The consequence of the blocks that are cryptographically allied is the attribute of immutability. The processing and organisation of the information or data associated with transactions in the block are accomplished using cryptographic principles [22]. Blockchain technology makes use of the Secure Hashing Algorithm 256 (SHA-256). A hash value that consists of an alphanumeric string is generated for each block. Blocks are established to be persistent and associated together retrospectively by the fact that each block comprises a digital signature or hash value for both itself and the block before it [22].

Blockchain is a type of distributed ledger technology that makes it conceivable to record transaction details instantaneously in diverse locations. Distributed Ledger Technology, unlike traditional databases, is not reliant on centralized administration since it was not premeditated with central data storage [23]. The Distributed Ledger's nodes independently verify and process each item to construct the consensus and

record of legitimacy. Cryptography is employed to safeguard the data retained on the Distributed Ledger. The ledger's structure has been constructed in a manner in which cryptographic hash functions integrate all of the nodes. Since the access method of Distributed Ledger is governed by cryptographic signatures and keys, the information's security and veracity are maintained. Applications-specific instructions are carried out via Smart Contracts on a typical Blockchain platform. Contrary to the consensus, this is not a contract in the traditional sense; rather, it is a set of instructions that has been put into operation. The self-execution and self-verification features of a smart contract can be equated to those of a computer program [24]. Any one or all of the peer nodes may host a smart contract because of its distributed and event-driven nature. The omission of any third party is made possible via a smart contract on the Blockchain, which makes the transactions autonomous. Trust obstacles can also be resolved considering there is no third party involved and transactions transpire only after the agreements are upheld.

5. Digital Identity

The concept of 'Identity' is theoretically complex. However, over the course of time, it has been characterized in numerous ways and situations. On a fundamental level, it can be argued that identity is any collection of traits that characterize an individual and can be used to specifically identify them. The digital equivalent of a person's physical identity, or the digital representation of the person, would be their digital identity as a result. According to National Institute of Standards and Technology guidelines, a digital identity is a grouping of distinctive features that distinguish an entity and specify the transactions in which it is permitted to engage [25]. The criteria for a standard digital identity include being distinct, created with the agreement of the user and verifiable with a high degree of certainty. The quantity of personal data organizations own about online consumers is expanding exponentially along with exponential technology. Organizations collect and absorb data without the users' acquaintance or consent, which is then used by third parties for data analysis, profiling, and other forms of exploitation [26]. One of the most crucial uses of Blockchain technology for numerous advancements is without any ambiguity managing and verifying digital identities. By keeping track of every transaction among identity holders and initiatives, the Blockchain ensures complete transparency at all times. The flexibility to generate an encrypted user identity that can be instantaneously accessible and used to validate identification as required is another benefit of Blockchain technology [27].

6. Smart City

The British Standards Institute defines a 'Smart City' as the efficacious incorporation of human, digital, and physical systems in the assembled settings to provide an ecological and comprehensive future for its residents [28]. The smart city is a concept that refers to the use of advanced technology and data analytics to improve the quality of life of citizens, enhance urban sustainability, and optimize the use of resources in urban areas [29]. Smart Cities integrate technology and data to manage assets, resources, and services efficiently while also promoting citizen participation and engagement. One technology that has been proposed as a potential enabler of smart

cities is Blockchain. This technology can be used to enable secure and transparent transactions between citizens and government entities in smart cities. By using Blockchain, smart cities can provide a decentralized and secure platform for citizens to interact with government entities, including paying taxes, applying for permits, and voting in elections [30]. One of the main applications of Blockchain in smart cities is in the area of identity management. In a smart city, citizens will interact with a range of services and systems that require identity verification, such as transportation systems, public services, and payment systems. Blockchain can provide a secure and decentralized platform for managing identity, allowing citizens to maintain control over their data and protect them from identity theft [31]. By leveraging the security and transparency of Blockchain, smart cities can enhance the trust of citizens in the data collected and analyzed, enable secure and transparent transactions between citizens and government entities, and create decentralized marketplaces for resources in urban areas.

7. Existing solutions

A system was suggested utilizing the Ethereum platform to contrivance a smart contract as part of a Blockchain-based solution for public procurement [32]. The contributors are permitted to submit bids using their suggested system after the organizer has instigated the procurement. This approach does, however, have a few flaws. The system's access control method is one of its key drawbacks. The highest bidder among the contributors is chosen if the Reveal function is called prior to the deadline expires, which also concludes the procurement. This, however, undermines the whole procedure because neither the winner nor the procurement can be terminated before the deadline. Another procurement mechanism was constructed on the Blockchain [33]. In contrast to the earlier approach, this solution offers faultless operation up until the point of procuring bids. This approach also contains a significant flaw. The probability of tender manipulation is substantial since the system allows the organizer to personally evaluate the submitted bids which also carries the risk of corruption. An alternative smart contract for public procurement was developed, and it was constructed in such a way that it can accomplish numerous requirements for public procurement [34]. However, the system's bidding function has a significant limitation. If a new contestant bids the identical amount as the in-progress highest amount, the offer will be rejected even though it is irrational and unfair. As a consequence of this, the system fails to uphold the fundamental requirement of impartiality in the procurement process.

8. Proposed solution

Due to the traditional centralized structure, typical public procurement is a protracted and complex process with a substantial opportunity for corrupt practice. The delinquent of third-party reliance, which conveys a number of unsolicited transparency difficulties, exist in any traditional procurement system with centralized architecture [35]. A Blockchain-based system with digital identification is suggested in light of the shortcomings of the existing systems outlined in this section.

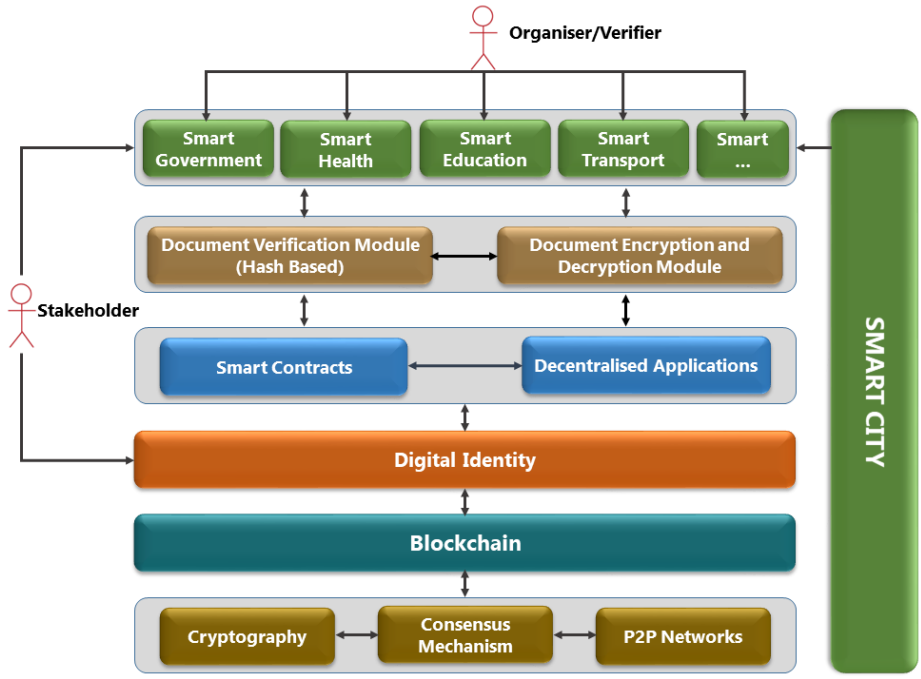

Fig. 3. Proposed Blockchain-based Solution Framework

The above figure illustrates the process of the system. The foundation layer comprises the peer-to-peer network, consensus mechanism and cryptography which provides the required decentralization and security needed to ensure transparency and trust in the process. Cryptography provides the necessary security by encrypting the data thereby preventing it from unauthorized access. The consensus mechanism safeguards that all the nodes on the network only approve the same request and the P2P network enables the direct communication between the nodes eliminating the middle tier. Above the foundation layer is the Blockchain layer which is the distributed ledger where all transactional data is stored and accessible by the stakeholders. It guarantees the traceability and transparency of the transactions and also provides the mechanism to detect any attempt to sabotage the data that has been stored on a tamper-proof and immutable distributed ledger. On top of the Blockchain layer is the Digital Identify layer in the framework where the identity of the stakeholder can be identified and validated preventing unauthorized access. Above the digital identity layer are the smart contracts and decentralized applications that are responsible for this function. Smart contracts are self-executing contracts whose terms and conditions are embedded in the code. These contracts provide leverage in automating the procurement process, including contract management, identity verification, payment processing and dispute resolution. On the other hand, decentralized applications can provide the user interface to interact with the Blockchain system. The top layer represents the elements of smart cities such as smart health, smart government, smart transport, smart education etc.

The suggested Blockchain-based solution will trigger the aforementioned procedure using smart contracts. Once the system is activated, the participant is allowed to register. Following the registration phase, the system issues a Digital ID to the participant which is required to submit the tender. The system will compare the current time to the submission deadline as the tender is being submitted. If the deadline has not passed, the participant may proceed with the submission. The subsequent phase of the process involves the system confirming whether or not the participant has already filed a tender. If no previous submission record exists, the relevant document will be encrypted followed by accepting the tender submission. However, the ability to submit a tender will no longer be available after the cut-off time. Once the deadline has passed, the documents will be decrypted. In the next phase, all of the bids will be evaluated and a winner will be declared according to the procurement policy. The Ethereum platform was chosen to create the Blockchain-based decentralized application. The Ethereum architecture makes it possible to express the network state using an account model [34]. Developers have the option to launch decentralized applications commonly known as DApps, on the Ethereum platform.

The following are some algorithms for the core functions of the solution.

Algorithm: Issue Digital Identity

```
FUNCTION generateDigitalIdentity(name, dateOfBirth, nationality, publicKey):
    digitalIdentityData = name + dateOfBirth + nationality + publicKey
    digitalIdentityHash = SHA256(digitalIdentityData)
    digitalIdentity = digitalIdentityHash
    emit DigitalIdentityGenerated(digitalIdentity)
END FUNCTION
```

This algorithm takes four input parameters - name, dateOfBirth, nationality, and publicKey - and combines them into a single string. It then hashes the combined string using SHA-256, which is a secure hashing algorithm. The resulting hash is stored on the Blockchain as a smart contract variable called digitalIdentity. Finally, the algorithm emits an event to indicate that a digital identity has been generated.

Algorithm: Encrypt Document

```
FUNCTION encryptDocument(document, encryptionKey):
    documentBytes = convertToBytes(document)
    encryptedBytes = encrypt(documentBytes, encryptionKey)
    encryptedDocument = encryptedBytes
    emit DocumentEncrypted(encryptedDocument)
END FUNCTION
```

This algorithm takes two input parameters - document and encryptionKey and converts the document into a byte array. It then encrypts the byte array using the encryptionKey, which could be a symmetric key or a public key if using asymmetric encryption. The resulting encrypted bytes are stored on the Blockchain as a smart contract

variable called encryptedDocument. Finally, the algorithm emits an event to indicate that the document has been encrypted.

Algorithm: Tender Submission

```
FUNCTION submitTimedTender(tenderDetails):
    require(isTenderSubmissionAllowed(), "Tender submission is not allowed at this time")
    require(isValidTenderDetails(tenderDetails), "Invalid tender details")
    require(now < submissionDeadline, "Tender submission deadline has passed")
    tenders.push(tenderDetails)
    emit TenderSubmitted(tenderDetails)
END FUNCTION
```

This algorithm takes one input parameter tenderDetails, which is a data structure containing the details of the tender submission. The algorithm first verifies that tender submission is allowed by calling a function isTenderSubmissionAllowed(), which could check criteria such as available budget. If submission is not allowed, an error is thrown. The algorithm then verifies that the tenderDetails are valid by calling a function isValidTenderDetails(tenderDetails), which could check criteria such as format, completeness, and eligibility. If the tender details are not valid, an error is thrown. Next, the algorithm verifies that the submission deadline has not passed by checking the current timestamp against a variable submissionDeadline which could be stored as a smart contract variable. If the submission deadline has passed, an error is thrown. If the tender submission is allowed, the tender details are valid, and the submission deadline has not passed, the algorithm adds the tenderDetails to the list of submitted tenders, which could be stored as a smart contract variable. Finally, the algorithm emits an event to indicate that a tender has been submitted.

Algorithm: Decrypt Document

```
FUNCTION decryptDocument():
    require(now >= submissionDeadline, "Tender submission deadline has not passed")
    require(!isDocumentDecrypted, "Document has already been decrypted")
    decryptedBytes = decrypt(encryptedDocument, encryptionKey)
    document = convertFromBytes(decryptedBytes)
    finalDocument = document
    isDocumentDecrypted = true
    emit DocumentDecrypted(document)
END FUNCTION
```

This algorithm assumes that the document has been previously encrypted using an encryption key and stored on the Blockchain as a smart contract variable called encryptedDocument. The algorithm first verifies that the tender submission deadline has passed by checking the current timestamp against a variable submissionDeadline

which could be stored as a smart contract variable. If the submission deadline has not passed, an error is thrown. The algorithm then verifies that the document has not already been decrypted by checking a boolean variable isDocumentDecrypted. If the document has already been decrypted, an error is thrown. If the tender submission deadline has passed and the document has not already been decrypted, the algorithm decrypts the encryptedDocument using the encryptionKey. The resulting decrypted bytes are then converted back to the original document. The algorithm then sets the document as the final document, which could be stored as a smart contract variable. The algorithm also sets the isDocumentDecrypted boolean variable to true to indicate that the document has been decrypted. Finally, the algorithm emits an event to indicate that the document has been decrypted.

Algorithm: Declare Winner

```
FUNCTION determineLowestBidder():
    require(now >= submissionDeadline, "Tender submission deadline has not passed")
    require(!isWinnerDetermined, "Tender winner has already been determined")
    lowestBid = tenderList[0].bid
    FOR i = 1 TO tenderList.length - 1:
        IF tenderList[i].bid < lowestBid:
            lowestBid = tenderList[i].bid
    lowestBidder = tenderList[0]
    FOR i = 1 TO tenderList.length - 1:
        IF tenderList[i].bid == lowestBid AND tenderList[i].compliance == true:
            lowestBidder = tenderList[i]
    finalTender = lowestBidder
    isWinnerDetermined = true
    emit TenderWinnerDetermined(lowestBidder)
END FUNCTION
```

This algorithm assumes that the tenders have been previously submitted and stored on the Blockchain as an array called tenderList. Each tender in the tenderList array has a property called bid which represents the price quoted by the bidder, and a property called compliance which represents whether or not the bidder meets the compliance requirements. The algorithm first verifies that the tender submission deadline has passed by checking the current timestamp against a variable submissionDeadline. If the submission deadline has not passed, an error is thrown. The algorithm then verifies that the winner has not already been determined by checking a boolean variable isWinnerDetermined. If the winner has already been determined, an error is thrown. If the tender submission deadline has passed and the winner has not already been determined, the algorithm determines the lowest bid by iterating through the tenderList array and comparing each bid to the current lowest bid. If a lower bid is found, the corresponding bid is stored as lowestBid. The algorithm then determines the tender with the lowest bid by iterating through the tenderList array again and checking if each bid is equal to the lowestBid and if the compliance property of the bidder is true.

If a tender meets these conditions, it is stored as lowestBidder. The algorithm then sets the lowestBidder as the finalTender, which could be stored as a smart contract variable. The isWinnerDetermined boolean variable is set to true to indicate that the winner has been determined. Finally, the algorithm emits an event to indicate that the winner has been determined.

9. Conclusion

The impartiality, openness, and dependability of the centralized structure raise questions that put the conventional procurement method in constant jeopardy. Numerous studies have revealed that it is challenging to set up a transparent and safe procurement strategy based on the conformist centralized architecture. This study detailed how Blockchain technology was applied to construct a trustworthy, secure, and transparent mechanism for the procurement process. The study highlighted the impediments to the conventional procurement model and elucidated its ineffectiveness. This paper evaluated the potential of Blockchain from the standpoint of mitigating procurement corruption through the functionality and usability of the technology. After evaluating the technology's potential in terms of its ability to track and regulate the transactions and records of any system at the ecosystem level, a decentralized application was generated. The decentralized platform has been reinforced by the Blockchain's physiognomies, which include transparency, immutability, security, and non-repudiation, protecting the procurement process from unlawful conduct.

References

1. What Is Procurement? https://www.investopedia.com/terms/p/procurement.asp, last accessed 2023/05/15.
2. Preventing Corruption in Public Procurement. http://www.oecd.org/gov/ethics/Corruption-Public-Procurement-Brochure.pdf, last accessed 2023/01/10.
3. Public procurement - Our priorities, https://www.transparency.org/en/our-priorities/public-procurement, last accessed 2023/02/01.
4. What Is Qualitative Research? | Methods & Examples, https://www.scribbr.com/methodology/qualitative-research/, last accessed 2023/03/15.
5. Punch, K.F.: Introduction to Social Research: Quantitative and Qualitative Approaches. (1998).
6. Edmonds, W.A., Kennedy, T.D.: An Applied Reference Guide to Research Designs: Quantitative, Qualitative, and Mixed Methods. (2012).
7. What is Procurement? https://www.hudsonprocure.co.uk/what-is-procurement-what-it-means-and-why-is-it-important-to-your-business/, last accessed 2023/01/19.
8. Uyarra, E., Flanagan, K.: Understanding the Innovation Impacts of Public Procurement. 18, 1, (2010). https://doi.org/10.1080/09654310903343567.
9. OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials, https://www.oecd-ilibrary.org/governance/oecd-foreign-bribery-report_9789264226616-en, last accessed 2023/01/20.
10. Curbing Corruption In Public Procurement: A Practical Guide, https://www.transparency.org/en/publications/curbing-corruption-in-public-procurement-a-practical-guide, last accessed 2023/04/03.
11. Digital Technologies for Transparency in Public Investment: New Tools to Empower Citizens and Governments, https://publications.iadb.org/en/digital-technologies-transparency-public-investment-new-tools-empower-citizens-and-governments, last accessed 2023/04/10.
12. Reuters | Breaking International News & Views, https://www.reuters.com/, last accessed 2023/01/15.
13. Shi, W. et al.: A Verifiable Sealed-Bid Multi-Qualitative-Attribute Based Auction Scheme in the Semi-Honest Model. 5, (2017). https://doi.org/10.1109/ACCESS.2016.2624558.
14. Pereira, J. et al.: Blockchain-based platforms: Decentralized infrastructures and its boundary conditions. 146, (2019). https://doi.org/10.1016/J.TECHFORE.2019.04.030.
15. Blockchain – the gateway to trust-free cryptographic transactions, https://aisel.aisnet.org/ecis2016_rp/153.
16. Bitcoin, Ethereum, Blockchain, Tokens, ICOs: Why should anyone care?, https://preethikasireddy.com/post/bitcoin-ethereum-blockchain-tokens-icos-why-should-anyone-care, last accessed 2023/05/16.
17. D'Angelo, G. et al.: A Blockchain-based Flight Data Recorder for Cloud Accountability. Presented at the June 15 (2018). https://doi.org/10.1145/3211933.3211950.

18. Biswas, S. et al.: Blockchain for E-Health-Care Systems: Easier Said Than Done. 53, 7, (2020). https://doi.org/10.1109/MC.2020.2989781.
19. Casey, M.J., Vigna, P.: Decentralized Blockchain Technology and the Rise of Lex Cryptographia. (2015). https://doi.org/10.2139/ssrn.2580664.
20. Biswas, S. et al.: GlobeChain: An Interoperable Blockchain for Global Sharing of Healthcare Data - A COVID-19 Perspective. 10, 5, (2021). https://doi.org/10.1109/MCE.2021.3074688.
21. Fung, A. et al.: Full Disclosure: The Perils and Promise of Transparency. 27, 1, 218–221 (2007). https://doi.org/10.1002/pam.20317.
22. de Leon, D.C. et al.: Blockchain: properties and misconceptions. 11, 3, (2017). https://doi.org/10.1108/APJIE-12-2017-034.
23. Lenz, R.: Managing Distributed Ledgers: Blockchain and Beyond. (2019). https://doi.org/10.2139/SSRN.3360655.
24. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things. 4, (2016). https://doi.org/10.1109/ACCESS.2016.2566339.
25. Grassi, P.A. et al.: Digital Identity Guidelines. National Institute of Standards and Technology (U.S.) (2017).
26. Maresova, P. et al.: Technological solutions for older people with Alzheimer's disease: Review. 15, 10, (2018). https://doi.org/10.2174/1567205015666180427124547.
27. Rathee, T. et al.: A systematic literature mapping on secure identity management using Blockchain technology. (2021). https://doi.org/10.1016/J.JKSUCI.2021.03.005.
28. PAS 181 The Smart City Framework - Smart City Concept Model, https://www.bsigroup.com/en-IN/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/, last accessed 2023/05/16.
29. Caragliu, A. et al.: Smart cities in Europe. 18, 2, (2011). https://doi.org/10.1080/10630732.2011.601117.
30. Böhme, R. et al.: Bitcoin: economics, technology, and governance. 29, 2, (2015). https://doi.org/10.1257/JEP.29.2.213.
31. Ferraro, P. et al.: Distributed Ledger Technology for Smart Cities, the Sharing Economy, and Social Compliance. 6, (2018). https://doi.org/10.1109/ACCESS.2018.2876766.
32. Chen, Y. et al.: Blockchain based smart contract for bidding system. 208–211 (2018). https://doi.org/10.1109/ICASI.2018.8394569.
33. Mali, D. et al.: Blockchain-based e-Tendering System. (2020). https://doi.org/10.1109/ICICCS48265.2020.9120890.
34. Kumar, B., Kumar, K.: Blockchain Based Smart Contract for Sealed-Bid Auction. (2019). https://doi.org/10.35940/ijeat.F8083.088619.
35. Yutia, S., Rahardjo, B.: Design of a Blockchain-based e-Tendering System: A Case Study in LPSE. (2019). https://doi.org/10.1109/ICISS48059.2019.8969824.