

# A Design of Blockchain Based Smart Contract for Tendering

Denies Kiyeng  
Department of Computer  
Science and Information  
Technology  
Kabarak University  
Nakuru, Kenya

Simon Maina Karume  
Department of Computer  
Science and Information  
Technology  
Kabarak University  
Nakuru, Kenya

Nelson Masese  
Department of Computer  
Science and Information  
Technology  
Kabarak University  
Nakuru, Kenya

---

**Abstract:** Information technology is the backbone for all 21<sup>st</sup> century organizations that are looking forward to offer better customer service and gain competitive advantage. Today, blockchain technology is being adopted by a number of organizations such as financial services, healthcare, agriculture and even government. . However, the tendering sector have not been able to take advantage of the new blockchain technology, owing to the absence of blockchain based frameworks and a model for secure tendering. This study focuses on block-chain with its BYOE (Bring Your Own Encryption) concept in the procurement sector. The research comes up with a design of a blockchain based smart contract model for organizations in Kenya following ASD approach. In addition a discussion of challenges and opportunities of Blockchain based tendering is also presented.

**Keywords:** model, blockchain, byoe, tendering, contract

---

## 1. INTRODUCTION

Blockchain is a decentralized public ledger based on P2P networks, which has attracted wide attention in distributed application systems in recent years (Guo, *et al.*, 2021). In this technology, a tamper resistant digital platform for data storage and sharing is realized by applying the chain-block structure and establishing a trusted consensus mechanism to synchronize data changes.

At the same time, the decentralization, traceability and immutability of on-chain information storage makes blockchain a trusted machine with high reliability and security (Wang, *et al.*, 2021). Based on these characteristics, researchers began to analyze the application of blockchain in various fields, such as the Internet of Things, supply chain management, voting system and bidding system. Blockchain in application can improve the availability of data and reduce costs, while maintaining the openness and transparency of the application (Wang, *et al.*, 2021).

Transparency is considered to be a prerequisite for ensuring the accountability of public officials and in regards, there is broad agreement that the effectiveness of transparency can be further strengthened by involving blockchain technology (Shin, and Ibahrine, 2020). Such technology could be effective in raising success, reducing risks in complex contracts, strengthening procurement and contracting practices, holding officials accountable and in general, strengthening supply chain process.

A blockchain-based solution is a good fit for use cases such as tendering where multiple parties having low levels of trust, transact with each other. The technology is applicable in areas where same transaction is stored across disparate systems or databases (Raj, *et al.*, 2018).

In recent years, electronic bidding has become an efficient and convenient service, which aims to provide an open and safe bidding environment for suppliers to protect the public interest (Wang, *et al.*, 2021). Tendering and bidding is a kind of commodity trading behavior which enables an organized selection of excellent transaction by the tendering organization. Compared with traditional offline bidding, it has an obvious difference in efficiency, in-formation collection and other aspects, and is better in the identity authentication of the bidding object, confidentiality of the bidding content, fairness of the bidding process and other aspects (Li, *et al.*, 2021).

Emerging blockchain technology combined with smart contracts could revolutionize traditional E-bidding systems in a decentralized and autonomous manner (Wang, *et al.*, 2021). It paves the way for a secure, immutable and auditable E-bidding process, while maintaining strong accuracy and completeness.

## 2. STATEMENT OF THE PROBLEM

The use of decentralized applications is poised to disrupt many sectors in the near future. Nonetheless procurement is among key areas still underserved by adoption of latest technologies such as blockchain. The Kenyan tendering ecosystems lacks behind because the technology is still new, having been introduced by Nskamoto (2008). Their exist possibilities that distributed applications Dapps are permeating to different sectors, tendering included. While the Dapp applications became much needed in Kenya, there is still absence of a clear framework and model to guide the realization of a blockchain based smart contract model for tendering.

## 3. STUDY OBJECTIVE

This research focuses on coming up with a design of a blockchain based smart contract model tailored to reduce

corruption in tendering while ensuring efficiency and openness.

### 3.1 LITERATURE SURVEY

A smart contract is a piece of self-executing code that can be stored, and executed, on the blockchain. A smart contract is deterministic, verifiable, and doesn't rely on any trusted third party. Entities can enter into an agreement with all of the terms transparent to them (Dannen, 2017). The same integrity checks that keep the transactions on the blockchain from being edited are also in effect here. This means that when entities enter into the agreement, they can be sure that no party will edit the terms of that agreement at a later date.

Smart contracts also have state and memory storage and so can hold assets in their own right. Implying that they can be used to hold funds in escrow in instances of asset transfer between parties (Sklaroff, 2017). The applicability of this goes far beyond the crypto-currencies that are currently popularizing the blockchain. The limitations of smart contracts are entirely in the expressiveness of the language supported by the blockchain (Primorac, 2016). With a Turing complete language, as is employed by Ethereum, smart contracts can be used to execute a number of functions. Therefore, smart contracts provide a trust less environment for asset exchange.

Blockchain-based smart contracts are proposed contracts that could be partially or fully executed or enforced without human interaction. One of the main objectives of a smart contract is automated escrow. An IMF staff discussion reported that smart contracts based on blockchain technology might reduce moral hazards and optimize the use of contracts in general. But "no viable smart contract systems have yet emerged." Due to the lack of widespread use their legal status is unclear (Wang, *et al.*, 2018).

Smart contracts are computerized transaction protocols that execute terms of a contract (Szabo, 2017). Smart contracts extended the functionality of electronic transaction methods, such as point of sale (POS), to the digital realm. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism (Mao *et al.*, 2018).

According to (Korpela, *et al.*, 2017) blockchain can have a significant impact on business, it can be a powerful tool in establishing trust. Blockchain based smart contract model for tendering process will ensure Greater transparency, Enhanced security, improved traceability, Increase efficiency and speed and reduced costs.

### 3.2 The Conceptual Design

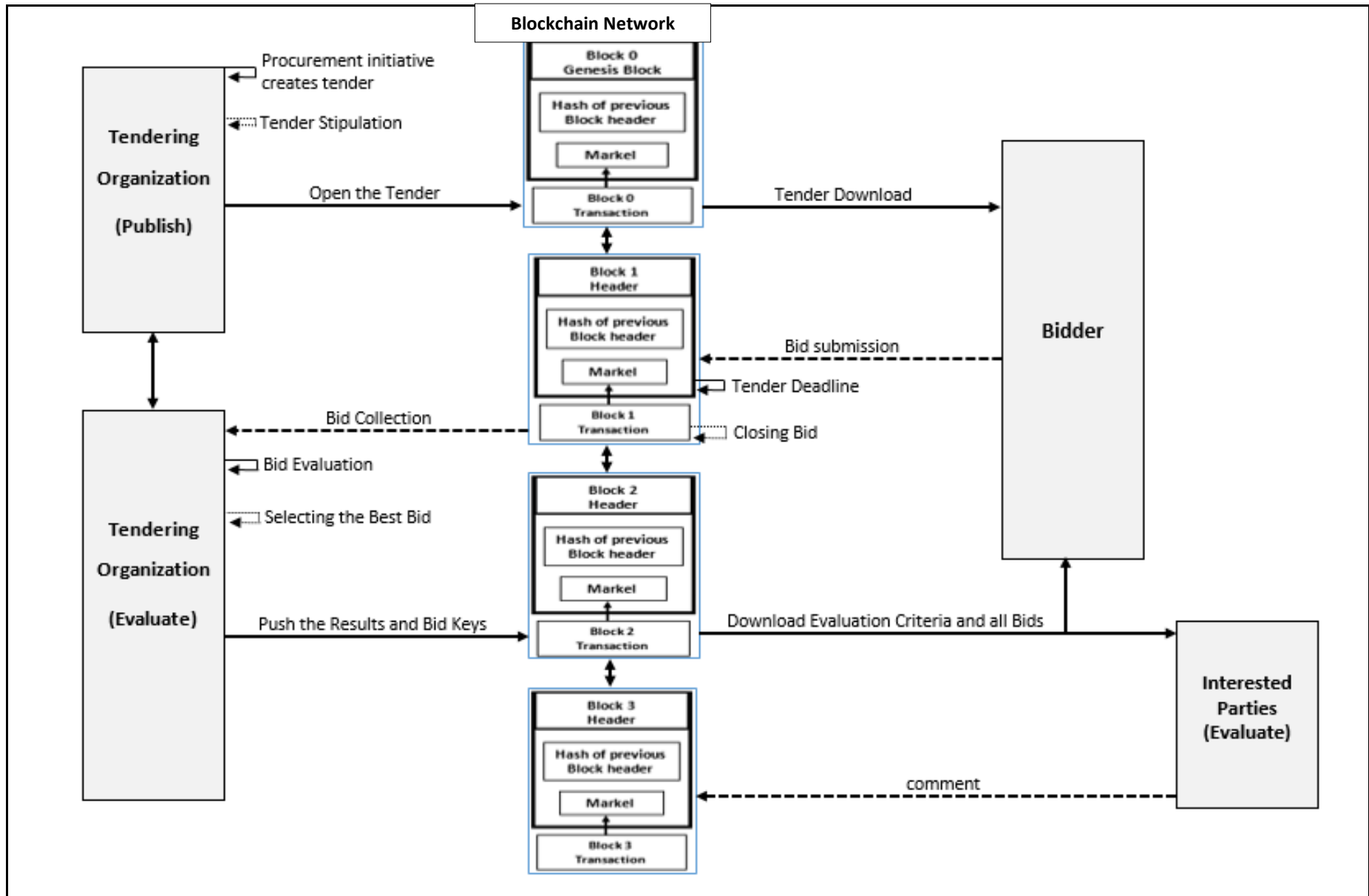
A tendering organization will create a tender as a smart contract and place it on the blockchain. The smart contract will include the certified public key of the tendering organization along with bid evaluation code. A prospective bidder can download the tender from the blockchain. The respective bidder reviews the tender and consider the tendering specification and make a bid proposal, then the bidder generates a bid in response to the tender (smart

contract). The actual bid is encrypted by the bidder's generated symmetric key (bid key: SKBidder).

The symmetric key is then encrypted by the public key of tendering organization: (SKBidder). Half of the (SKBidder) is included as part of the submission and the second half would be communicated to the tendering organization at the tender submission deadline. The bidder will push the bid as a smart contract to the blockchain. The bid is signed by the bidder's certified signature key. This key is certified by the tendering organization when the bidder register as an authorized bidding company - a process out of the actual tender opening and allocation process

When the deadline for bid submission expires, the smart contract on the blockchain stops accepting new bids. The tendering organization can download the submitted bids, and they can decrypt the bids if they have full (SKBidder). At the tender closing date, tendering organization will run the evaluation code and select the best bid. The result of the evaluation is pushed to the blockchain. At this stage, the tendering organization can make (SKBidder) of all bidders public on the blockchain. The illustration of the working concept of the blockchain model for procurement is illustrated in figure 1 below.

The tender organization will push the results of the bid evaluations along with bidder's keys to the blockchain. This information is crucial for independent auditing of the tendering process. Interested parties can access the tender details from the blockchain (where this data will reside in perpetuity) along with the bid evaluation code. Interested parties can download the tender contract that contains the code for bid evaluation criteria. Interested parties just have to run the evaluation code that will read the bids from the block and evaluation them. The results of the evaluation will show whether the bidding process was fair (auditing tender allocation to the stated best bidder)



#### 4. ASSUMPTIONS

For parties to be involved in monitoring the organization activities, they need efficient tools and intuitive assessment that gives clear results. To build such an environment, blockchain and smart contracts show great potential. In this research the tendering process is will be implemented in the blockchain environment to provide an open and fair tendering scheme.

The design outlined is limited to four standard users: Admin, Biding organization, Bidder, and Third parties. In order to describe the various functional requirements that users have on the model, user stories from a focused group need to be written. The user stories need to be simplified to the bare minimum requirements, while still keeping the PoC at a viable level of usability and security.

#### 5. RECOMMENDATION

The Government should move towards creating a legal framework for Ethereum and other digital currencies. Although many governments as shown in the literature are now considering launching their own Bitcoin-like cryptocurrency, the process should include sensitizing citizens and financial organizations. This will in addition encourage adoption of the blockchain based smart contracts model for tendering process among organizations.

#### 6. CONCLUSION

For parties to be involved in monitoring the organization activities, they need efficient tools and intuitive assessment that gives clear results. To build such an environment, blockchain and smart contracts show great potential. In this study, the tendering process will be implemented in the blockchain environment to provide an open and fair tendering scheme.

- [1] Guo, Y. (2010, August). E-government: Definition, goals, benefits and risks. In 2010 International Conference on Management and Service Science (pp. 1-4). Ieee.
- [2] Guo, Y. M., Huang, Z. L., Guo, J., Guo, X. R., Li, H., Liu, M. Y., ... & Nkeli, M. J. (2021). A bibliometric analysis and visualization of blockchain. *Future Generation Computer Systems*, 116, 316-332.
- [3] Wang, J., & Lei, C. (2018). Will Innovative Technology Result in Innovative Legal Frameworks? – Smart Contracts in China. *European Review of Private Law*, 26(6), 921-942.
- [4] Wang, Y., Yang, B., Liu, J., Zeng, H., & Xia, C. (2020). Virtual chain: A storage model supporting cross-blockchain transaction. *Concurrency and Computation: Practice and Experience*, e5899. (Li, et al., 2021).
- [5] Li, X., Wang, Z., Leung, V. C., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered Data-driven Networks:

A Survey and Outlook. *ACM Computing Surveys (CSUR)*, 54(3), 1-38.

- [6] Sklaroff, J. M. (2017). Smart contracts and the cost of inflexibility. *U. Pa. L. Rev.*, 166, 263.
- [7] Primorac, J. (2016, September). Labour Practices in the Audiovisual Industry: The Impact of Virtual Work in Runaway Productions. In *ESA RN18 Mid-Term Conference'Rethinking Power in Communicative Capitalism*. Critical Perspectives on Media, Culture and Society'.
- [8] Korpela, K., Hallikas, J., & Dahlberg, T. (2017, January). Digital supply chain transformation toward blockchain integration. In proceedings of the 50th Hawaii international conference on system sciences.
- [9] Dannen, C. (2017). *Introducing Ethereum and Solidity*. Berkeley: Apress.
- [10] Mao, D., Hao, Z., Wang, F., & Li, H. (2018). Innovative Blockchain-Based Approach for Sustainable and Credible Environment in Food Trade: A Case Study in Shandong Province, China. *Sustainability*, 10(9), 3149. (No. PRC 17-84 F). Texas A&M Transportation Institute.
- [10] Makupi D., (2020). 5G Propelled AI, IoT and Blockchain: international Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 9, Issue 5, May 2020, ISSN: 2278 – 1323.