A BLOCKCHAIN BASED SMART CONTRACT MODEL FOR TENDERING

KIYENG KIPKEMOI DENIS

A Thesis Submitted to the Institute of Postgraduate Studies in Partial Fulfillment of the Requirements for the Award of Master of Science in IT Security and Audit Degree.

Kabarak University

NOVEMBER 2022

DECLARATION

I do declare that:

1. i) This thesis is my own work and to the best of my knowledge, it has not been presented for the award of a degree in any university or college.

   ii) The work has not in-cooperated material from other works or a paraphrase of such material without due and appropriate acknowledgement.

   iii) The work has been subjected to processes of anti-plagiarism and has met Kabarak University 15% similarity index threshold.

2. I do understand that issues of academic integrity are paramount and therefore I may be suspended or expelled from the University or my degree may be recalled for academic dishonesty or any other related academic malpractices.

Signature ……………………………………… Date ………9/11/2022**……..**

Denis K. Kiyeng

GMI/NE/0824/05/16

RECOMMENDATION

This thesis entitled **"A BLOCKCHAIN BASED SMART CONTRACTS MODEL FOR TENDERING PROCESS."** and written by Denis Kiyeng is presented to the institute of postgraduate studies and research of Kabarak University. We have reviewed is thesis and recommended it be accepted in partial fulfillment of the requirements for the degree of Master of Science in information technology.

Signature ……………………………………………..……   Date ………08/11/2022……….

Prof. Simon Karume

Department Science Engineering and Technology

Kabarak University.

Signature ………..…………………………….………   Date ………08/11/2022……….

Dr. Nelson Masese

Department Science Engineering and Technology

Kabarak University.

ACKNOWLEDGEMENTS

First, I would like to thank God for His guidance and strength during this study. I would also like to pass my gratitude to my supervisors Prof. Simon Karume of Kabarak University and Dr. Nelson Masese of Kabarak University, Department of Science Engineering, and Technology for their guidance and tireless efforts during this study. I sincerely thank Kabarak University for the conducive environment and for this opportunity to further my education.

Many thanks go to the members of the Department of Science Engineering and Technology Kabarak University for sharing selflessly their scholarly and scientific experiences.

I am also very grateful to my family and colleagues for their continued support and patience while undertaking this study.

DEDICATION

I dedicate this thesis to my parents Mr. Emmanuel Songol and Mrs. Salina Songol who have always loved me unconditionally and whose good examples have taught me to work hard for the things that I aspire to achieve; they have greatly taught me that even the biggest assignment can be accomplished if done a step at a time. It is also dedicated to my friends Dr. Daniel Makupi, Alex Kibet, Anthony Musabi, Patricia Chebet, Joshua Mutai, Laurence Siele, John Langat, and Evans Chesang who have always been a constant source of support and encouragement during the challenges of my academic life. Also to my brother Dominic Kiyeng and Sisters Marine and Mercyline who I am truly grateful for being in my life. This work is also dedicated to all those who might find it useful.

ABSTRACT

Information technology is the backbone for all 21^{st}-century organizations that are looking forward to offering better customer service and gaining a competitive advantage. Today, the blockchain technology is being adopted by several organizations such as financial service providers, healthcare, agriculture, and even government sectors. Nonetheless, the procurement sector has adopted information technology in its processes especially with the advent of E-procurement technology. However, the tendering sector has not been able to take advantage of the new blockchain technology. This study focuses on the blockchain and its BYOE (Bring Your Own Encryption) concept in the procurement sector. Using a proof of concept approach the research came up with a blockchain-based procurement model for organizations. The model was designed following ASD approach. While Ethereum based solidity smart contract with Truffle running on 127.0.0.1:9545 and MetaMask installation was configured for the running environment. In addition, Ganache running on localhost 127.0.0.1:7545 for the graphical interface was realized. The running hosted model is available at https://gov.chimera-iot.co.ke/index.php. The model prototype was evaluated based on the model goals and software quality attributes. Software quality attributes, was a purely technical evaluation that used test cases to see if the model requirements were attained. To ascertain the model goals, the evaluation intended to identify issues related to the various model components and gauge user experience. At the end of the evaluation process, the functional testing proved that all the model functional and system requirements were satisfied. The feedback from the users also indicated that most of the participants were able to accomplish all the model functionalities. Participants also strongly agreed that the model satisfied all the goals and software quality attributes. The model verification and validation results showed that the model design satisfied all the intended objectives. The model was able to automatically initiate the tender, place bid and perform bid evaluation & relay bid results with relevant bid reports. The functional model was able to provide transparencies by ensuring bids are not concealed and ensuring immutability of transaction thus ensuring transparency and openness. The overall idea was therefore found to be feasible and practical.

Keywords: *Blockchain, Smart contract, Ethereum*

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ASD	Adaptive software development
BTP	Bit-property
DLT	Distributed ledger technology
EVM	Ethereum Virtual Machine
E-GPS	E-Government Procurement systems
GOK	Government of Kenya
ID	Identification
OCDS	Open Contracting Data Standard
POC	Proof of concept
POS	Point of sale
APP	Application
e-GP	Electronic-Government Procurement
WTS	Web-based Tendering System
MB	Mega Byte
DApp	Decentralized applications

OPERATIONAL DEFINITION OF TERMS

Blockchain A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions. Constantly growing as 'completed' blocks (the most recent transactions) are recorded and added to it in chronological order, it allows market participants to keep track of digital currency transactions without central recordkeeping. Each node (a computer connected to the network) gets a copy of the blockchain, which is downloaded automatically.

Ethereum Network Ethereum is a decentralized platform that runs smart contracts**:** applications that run exactly as programmed without any possibility of downtime, censorship, and fraud, or third-party interference.

Smart Contract Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. 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. They render transactions traceable, transparent, and irreversible.

Solidity Solidity is a contract-oriented, high-level language for implementing smart contracts. It is designed to target the Ethereum Virtual Machine (EVM)

Ethers Ether is the integral element of the Ethereum blockchain network that acts as the network's fuel, keeping it agile and functional. While many believe that ether is the native digital currency of Ethereum, it acts as a medium of incentive or form of payment for the network participants to execute their requested operations on the network.

Model Is a program that runs on a computer that creates a model, or simulation, of a real-world feature, phenomenon or event.

CHAPTER ONE

INTRODUCTION

1.0 Introduction

This chapter provides a background of the study. It further continues to outline the research objectives, listing the research questions, states the research problem, and defines the scope, assumptions, significance as well the contributions of the study.

1.1 Background to the Study

The world businesses order is changing at a fast pace, business entities are reengineering their business processes and improving the efficiency of operations. The essential concept about having non-immutable transactions will redefine the distributed ledger landscape determining who controls or leverages the opportunities brought by the new technology infrastructure. More so, with the ever-increasing space of emerging technologies in the cyber space realm. Soon, the competitiveness of how businesses are connected is going to depend on the type or speed at which they integrate new technology. Organizations will be gaining a differentiating factor from each other depending on how they invest in the blockchain and related emerging technologies.

Procurement and tendering should be conducted in a fair, open and transparent manner (Olatunji, et al., 2016). The most important and broadly accepted principle underlying a modern procurement system is open competition to the procurement market. In addition, the tendering procedure should be open to public examination and review, thus making it a transparent process (Erdmenger, 2017). Procurement and tendering being a key integral to output of the business, it should be conducted in a transparent manner. As the society's values have shifted, there is necessity for transparent and fair manner of conducting tendering process (Ameyaw, et al., 2015).

The overall research problem addressed in this study is that despite an increase in knowledge in the tendering processes in organizations, very little has been done to realize openness, accessibility, integrity, fairness, inefficiencies, delays, transparency and profitability in the tendering process (Häkkinen, et all 2015). In 2015, in respect of all these the GOK began implementing reforms to address inefficiency in the use of Public resources and weak institutions of governance. The reforms included the development of anti-corruption strategies to facilitate the fight against corruption and the enactment of the Public Officer Ethics Act 2020, the Ant-Corruption and Economic Crime Act, the Financial Management Act 2020, and the Public Procurement and Disposal Act 2020 (Keyter, 2016). The aim was to make the procurement process more transparent, ensure accountability and reduce wastage of public resources among others.

Currently, there is lack of transparency, poor linkages between procurements and expenditures, delays and inefficiencies, poor records management, bureaucracy, rampant corruption, Political interests, hence the need for new technology like blockchain in tendering process to improve the overall performance in procurement (Ashworth, et al., 2018).

The existing systems have had institutional weaknesses that not only undermine their capacity for carrying out their mandates effectively but also have led to a Public perception that the Public sector was not getting maximum value for money spent on procurement (GOK, 2010). In view of the above shortcomings, this study found it necessary to have blockchain technology to ensure that all procurement entities attaining the objectives of an open and fair tendering process in an organization.

The decentralized ecosystem offered by blockchain is based on P2P networks. Which has attracted wide attention in distributed application systems in recent years (Guo, *et al*., 2021). It provides a tamper-proof resistant digital platform by applying the chain-block structure and establishing a trusted consensus mechanism to synchronize data changes. At the same time, the decentralization, traceability, and non-immutability of on-chain information storage make blockchain a trusted machine with high reliability and security (Wang, *et al.*, 2021).

Already working use cases have been realized in various fields, such as the Internet of Things, supply chain management, and voting system. It has been proved that applications based on Blockchain can improve the availability of data and reduce costs while maintaining the openness and transparency of the application (Wang, *et al.*, 2021).

Its implementation in procurement is poised to ensure the accountability of public officials (Shin, and Ibahrine, 2020). Therefore organizations, using these techniques will realize success, reduce risks in complex contracts, strengthen procurement and contracting practice while holding officials accountable, and in general, strengthen the tendering process. Additionally, it provides a procurement infrastructure that is more open to competition through public examination and review, thus making it a transparent process (Erdmenger, 2017).

In recent years, many governments emphasize on organizations and public entities to adopt Electronic bidding (E-bidding), with the core aim of ensuring an open and safe bidding environment (Wang, *et al.*, 2021). In 2020, the Government of Kenya published the public procurement and asset disposal regulation providing detailed guidance and elaborate procedures for the establishment and use of e-procurement systems.

It is, therefore, primetime for organizations as it re-engineer their processes by integrating blockchain technology. Not long, it will be supporting a bigger number of business use cases in diverse industry operations. As blockchain is expanding, more customers can realize its flexibility and positive impact as it powers up many enterprises.

1.2 Statement of the Problem

The tendering process is vital for stakeholders, especially when it can be traced later after bid closure. Tendering inefficiencies cost organizations a huge chunk of cash in delayed purchases, missed discounts, and transaction disputes (Åkers, 2018). The working procurement ecosystem currently is based on paper and tender boxes. It depends on the goodwill of tendering department because the outsiders are locked out from participating during the entire process of receiving bids. There is no working mechanism to establish a secure digital infrastructure that deters the tendering organization from trapping the bids inside the business process. Hutchinson (2015) also agrees that regardless of more elaborate tendering rules, still corruption and manipulation continue to degrade the entire tendering process due to the lack of a tamper-proof model and framework in place. On the other hand, modern businesses integrate blockchain to establish trust-based technology mechanisms (Korpela, *et al.*, 2017). Nevertheless tendering still lacks a model based on Blockchain Smart Contract that has a tool to establish trust.

1.3 Objective of the Study

1.3.1 Main Objective

The main objective for this research was to design a blockchain-based smart contract model tailored to reduce corruption in tendering while ensuring efficiency and openness. The design of the said model was guided by the following specific objectives;

1.3.2 Objective of the Study

i. To investigate existing weaknesses of e-tendering systems.
ii. To design a blockchain-based smart contract model for tendering.
iii. To develop the prototype of a blockchain-based smart contract model for tendering.
iv. To validate the blockchain model for tendering.

1.4 Research Questions

i. What are the weaknesses of e-tendering systems?
ii. How will the blockchain-based smart contract model for tendering be designed?
iii. How will the prototype blockchain-based smart contract model for tendering be implemented?
iv. How will blockchain model for tendering be validated?

1.5 Justification of the Study

The model design feature of using peer-to-peer network and blockchain for smart contract transaction provide potential opportunities in tendering. It offers a possible solution to the current problems of frauds and corruption during tender awarding process. This, therefore, is projected to provide a digital and alternative solution in ensuring transparency and fairness in tendering ecosystem.

Much effort by stakeholders and partners has yielded little in reducing frauds and corruption that has always confronted tendering in developing countries. Without trust and transparency, vast amounts of value are trapped and soloed inside the business processes of an organization. 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 as well reduce costs and thus therefore provide a milestone to procurement officers, auditors, anti-corruption agencies, and any other who will find the model relevant. Relying on Paper-driven tendering process has a cascading effect on an organization’s bottom line. A routine purchase generates bundles of paperwork and needs too many back-and-forth emails to set things straight. Tendering inefficiencies cost organizations a huge chunk of cash in delayed purchases missed discounts and transaction disputes.

1.6 Expected Outcome of the Study

The results of this research came up with the following deliverables;

i. Report on the weakness of e-tendering systems.
ii. Model design for blockchain-based smart contract model for tendering.
iii. Prototype of a blockchain-based smart contract model for tendering.
iv. Report on test and validate of blockchain for tendering prototype.

1.7 Scope of the Study

This study focused on the development of an application model for tendering with a blockchain-based smart contract, which provided non-repudiation, collision avoidance, confidentiality, and integrity along with independent auditability features and evidential guarantees. It did not overlap with already existing models towards tendering processes. However, the study did not concentrate on crypto-currency, block mining process, procurement governmental stand, rather it focused on a blockchain-based smart contract model to automate and bring openness in tendering. Also, this model did not force on the other components of procurement procedures like payment and work done but only on tendering actions. Finally, this study limited its geographic scope to Kenya, this brought efficiency leading to success in achieving the objectives of the study.

1.8 Limitations of the Study

Frequent updates of solidity environment, dependencies, and development tools without backward compatibility were a big challenge. To overcome this limitation, this study was limited to studying and implementing blockchain technologies in an Ethereum virtual machine platform. The Ethereum Virtual Machine platform supports the creation of decentralized applications (DApps) and manages accounts as well as smart contracts.

1.9 Assumptions of the Study

This study assumed that it got maximum cooperation from the organization's procurement department to implement a blockchain-based smart contract model for tendering to realize its full functions and benefits.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter explores existing related work and presents a critical appraisal of prevailing studies to identify the research gap. The first section presents the factors that affect transparent tendering processes. It goes ahead to deliberate on the blockchain technology and how it can transform procurement and tender, it extends to discuss the existing smart contract models and Blockchain benefits. In the last section, prototype development is discussed, also the conceptual framework and theoretical perceptions for the study are presented and discussed.

2.1 Procurement and Tendering

Tendering is the process of finding and agreeing to terms for acquiring goods, services, or works from an external source, often via a tendering or competitive bidding process, by which bids are invited from interested parties (Liao, *et al*., 20018). Tendering should adopt and observe the key values of fairness, clarity, simplicity, and accountability, as well as reinforce the idea that the apportionment of risk to the party best placed to assess and manage it is fundamental to the success of a project (Armstrong, *et al*., 2017).

The two most commonly used methods of tendering are single-stage selective tendering or two-stage selective tendering. Both involve the invitation of tenders from firms on a pre-approved or ad hoc list, chosen because they meet certain minimum standards in general criteria such as financial standing, experience, capability, and competence. The competition element of the tender is provided based on price and quality (Kumra, *et a*l., 2012).

2.2 Weakness of Existing e-tendering Systems

To raise the prominence of technology, it needs to be a reason for the technology to exist. E-tendering is the shift from the traditional paper-based system to the electronic system in bidding, which requires high technical capabilities from the procurement management staff, as well as advanced knowledge of communication technology and the internet. Therefore, to defend the need for a new blockchain smart contract, the existing real-world alternative needs to exhibit inefficiencies in their use cases (Larrucea, & Pautasso, 2020). That is why blockchain technology is rapidly hitting the mainstream, from a fit assessment framework for blockchain use cases report, it points out that blockchain-based solution is a good fit for tendering due to multiple parties having low levels of trust and transacting with each other. It also indicates that the technology is applicable in areas where the same transaction information is getting stored across disparate systems or databases (Li, *et al*., 2019). The following are existing e-tendering systems for tender management.

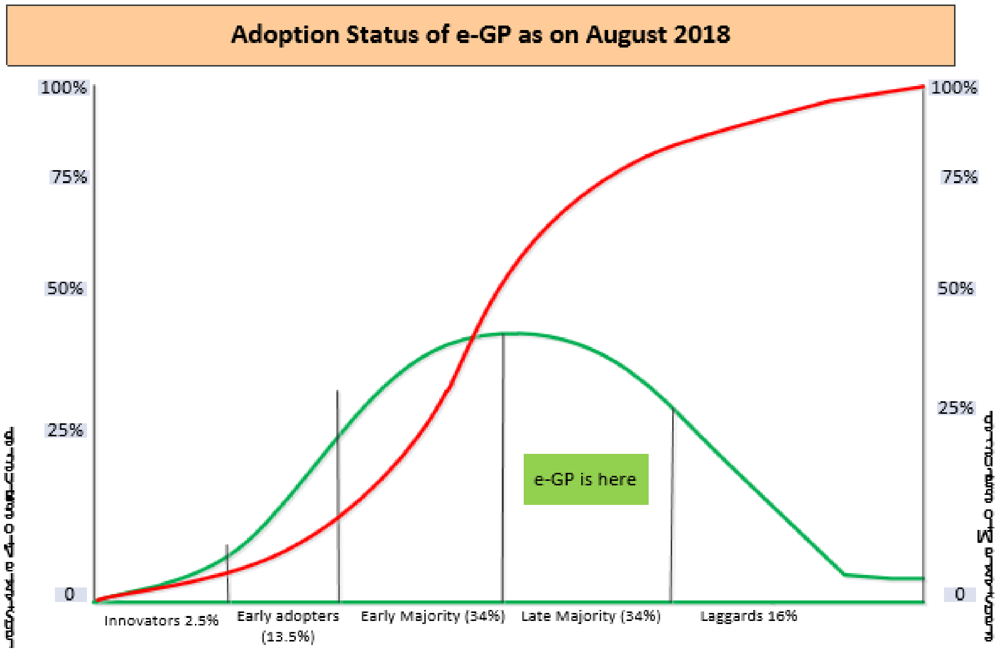
2.2.1 Global e-Government Procurement System

E-Government Procurement systems (e-GP) have been operational for close to 2 decades now. Many countries in America, Europe, and Asia Pacific have adopted e-GP, and countries in the African region are now getting on-boarded. Biswas (2015), Stated that the number of e-GP installations worldwide is in the range of 200 – 250. It is just a question of time before closing to 100% of the countries will have adopted e-GP and almost all the government procurement will happen online in e-GP.

The adoption of e-government procurement (e-GP) is now widespread across the globe. It can be said that e-GP as innovation has reached the late majority phase in the diffusion of innovations model. Refer to the Figure below for a pictorial view on the adoption status of e-GP as of August 2018 (Rahman, 2015).

Figure 1

Enhanced efficiency and transparency graph (Rahman, 2015).



Though the implementation of e-GP systems has contributed to enhanced efficiency and transparency in government procurement, there is potential for further advancement of the existing systems. Unless the many e-GP systems are made interoperable, Governments and the supplier community will not be able to realize the full benefits of e-GP. Hence, a mechanism is required to enable at least data level if not process level inter-operability among the multiple e-GP systems (Tran, *et al.*, 2011).

The key data level inter-operability requirements are:

i. A de-duplicated supplier database with each supplier distinctly identified across all the e-GP systems.
ii. Authenticated work experience certificates consolidated directly from multiple e-GP systems using Open Contracting Data Standard (OCDS).

Of the 2 requirements listed above, the establishment of a de-duplicated supplier database is the most critical and also the most difficult to implement. When a supplier can be distinctly identified across e-GP systems, it is relatively easier to consolidate authenticated work experience data of suppliers from multiple e-GP systems.

The e-GP Blockchain network should be extended to enable Banks located anywhere in the world to seamlessly submit authenticated Electronic Performance Bank Guarantees on behalf of a supplier in any of the networked e-GP systems (Neupane, *et al.*, 2014).
The key design principles underlying the global e-GP architecture are:

(i) Build on existing e-GP systems.

(ii) Incentivize de facto adoption of standards.

(iii) Open network with minimal entry barriers.

(iv) Near zero transaction costs.

It is proposed to implement the envisaged global e-GP architecture using Blockchain technology. The e-GP Blockchain is envisaged as a public network.

2.2.2 Web-based Tendering System for e-Government Procurement

Santos (2022) says e-Government uses improved Internet-based technology to make it easy for citizens and businesses to interact with the government, streamline processes, and improve citizen-to-government communications. The goal of these initiatives is to eliminate redundant systems and significantly enhance the government's quality of customer service for citizens and businesses.

One of the application domains of e-Government initiatives would be on G2B where government departments procure goods or services from the supplier via open tendering or other means (Malodia, *et al.*, 2021).

E-Tendering in a general sense fits under such a plan of e-Government initiative that adds values to trading parties by using Internet technology by facilitating their procurement process for both procurer and supplier. The goal is to improve the productivity and effectiveness of various business processes is in facilitating the trading amongst business partners and government agencies (Mc Loughlin., *et al.*, 2021).

Chan (2022) observes that e-Tendering service has evolved progressively over the years from online information browsing to integrated business solutions. They can be approximately classified into the following four groups which are also seen as a roadmap of evolution.

Table 1

Changes in the e-Tendering website over the years (Al-Bishari, et al., 2021).

In the 1980's	One-way information push
In the 1990's	Two-ways information push and pull
In the 2000's	Partially integrated system
Now and beyond	Fully integrated system

In principle, e-Tendering systems are about using technology to their fullest to provide services and information that is centered on facilitating information search, tender creating, tendering process, bids evaluation, and selection, etc. (Al-Bishari, *et al.*, 2021).
In the early 1980s, the efforts were pioneered in digitizing the tender information and displaying them on a website as a bulletin board, usually in the form of notices. The e-Government website (of which the Tendering Notice) served as an alternative platform for information display in addition to the traditional method of publishing in Gazettes (Al-Bishari, et al., 2021). Interested suppliers from the public who want to participate in the tendering would have to follow up via human contacts such as phone calls and in-person interviews. All subsequent processes were to be carried out manually and paper-based to close the loop. In the latter years, the usage of the website was extended to allow files that were digitized from paper documents to be downloaded, and online forms can be filled in and submitted online. Some enabled users to pay for the application fees online too, with transactional payment abilities.

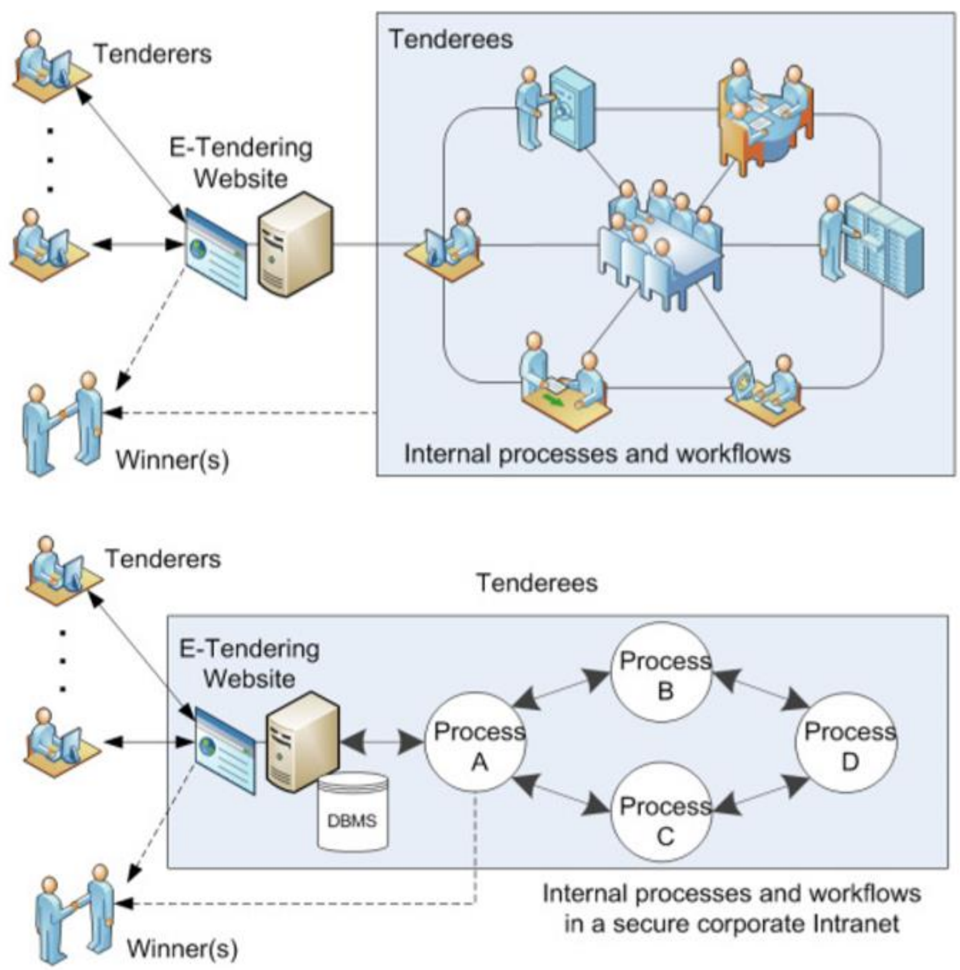
Figure 2 shows a scenario where the so-called Web-based Tendering System (WTS) or e-Tendering was mainly used for information display on a website. While most of the front end
 services that interact with the users

(suppliers) are digitized, a large part of the backend processes remained unchanged (Al-Bishari, et al., 2021).

It is known that reforming processes and workflows especially in a bureaucratic environment like government bodies involves many policy issues and would have to gradually take time (Maulana, et al., 2022). The backend processes are core functions of e-Tendering that include but are not limited to the following: tender creation, bids evaluation, policy making, decision making, and other supports.

Figure 2

E-Tendering system with mainly offline processes (Al-Bishari, et al., 2021).



E-Government efforts progressed eventually into digitizing both the information and services of both frontend and backend. At the turn of the millennium, the backend processes were partially integrated with automated workflows. They are more or less digitized and operate in a secure Intranet environment mainly for exchanging and archiving documents. This describes WTS in most e-Government situations nowadays – the front end is largely used for interacting with users and the backend is partially automated and integrated (Al-Bishari, et al., 2021). The scenario of today's WTS is reflected in Figure 3 and maybe a hybrid of Figures 2 and 3. Figure 3 shows an ultimate scenario which may be the final goal of e-Government reform that the processes are fully integrated and automated. The whole WTS is unified by closely coupling the website and the backend workflow as a whole application.

WTS can help substantially in migrating some manual processes in the backend to the web-based internal process by automating the bid evaluation, decision support for selecting the winner, and others (Al-Bishari, et al., 2021). The architecture of the WTS design is modular, hence it is possible to incorporate additional backend processes that eventually lead to a fully unified integration.

2.2.3 E-tendering System in Kenya - Focweb

The E-tendering system is dynamic web procurement and tendering system in Kenya that allows contractors to bid for tenders online (Mutangili, 2019). The system facilitates the application of tenders online and provides a dynamic secure backend platform for the management and awarding of the tenders. This system has successfully been piloted and used in a government state agency. The system can be used by any organization be it government institutions or private companies (Bharosa, *et al.*, 2020). This model is intended to reduce cost in the case that it reduces the paperwork used in the manual system; it also reduces the transport cost of the bidder since they can bid online.

The governors have identified a number of problems with the system. It has recentralized procurement and contributed to marginalization of locals in tendering. People and businesses that do not have access to the Internet cannot take part in the supplier selection and contracting process at county level (Guo, et al., 2022).

There have also been problems with malfunctioning of the system, to the point where counties have been unable to promptly pay bills to suppliers, causing problems for those firms and creating a crisis of confidence in the process (Guo, *et al.,* 2022). There are also issues with the infrastructure that is needed to support electronic procurement. In some cases, the system has had very limited availability, one county was allowed to access the system for two hours only in two weeks.

Now some observers see this as a push-back against the anti-corruption aspect of the system. But the government does need to show that it is doing everything possible to make this a success, and these do seem to be fundamental issues. The most important point is that it is not enough to just have a system. It is (as we mathematicians say) a necessary but not sufficient condition for achieving successful e-procurement. So whatever happens next in Kenya, we can see that having the technical infrastructure for e-procurement is vital. A reliable Internet service that can be accessed reliably by the supply market is essential if this to work well (Akram, *et al.,* 2021).

2.2.4 E-Tendering System – e-PPS

E-PPS is a web-based, collaborative system to facilitate the full lifecycle of a tendering process, for both buyers and suppliers. It offers a secure, interactive, dynamic environment for procurements of any nature, complexity, or value, enforcing (where appropriate) and encouraging recognized best practices (Nyaberi, 2020).

E-PPS supports the process of procuring works, services, and supplies electronically. Different public procurement procedures are supported for both one-off or repetitive purchases through several dedicated sub-modules providing facilities for user registration, competition notification, bid preparation and submission, online bid evaluation, contract awarding, creation and management of catalog-based information, placement of electronic purchase orders, electronic Invoicing and order tracking (Ahmad, *et al.*, 2019).

Unfortunately, e-Tendering system practices have some limitations and risks such as: The total cost (TCO) may be too high. It may be subject to hacker attacks due to its nature of database being centralized. Also it may be difficult to get suppliers to cooperate electronically (Al-Bishari *et al.,* 2021). The system may be too complex (e.g., when it uses a traditional EDI). E-Tendering portray difficulty in having internal and external integration (sometimes it involves different standards). As technology may change frequently, tendering is an extremely important success factor for many companies. Therefore, it is important to learn about the future of e-tender (Al-Bishari *et al.,* 2021).

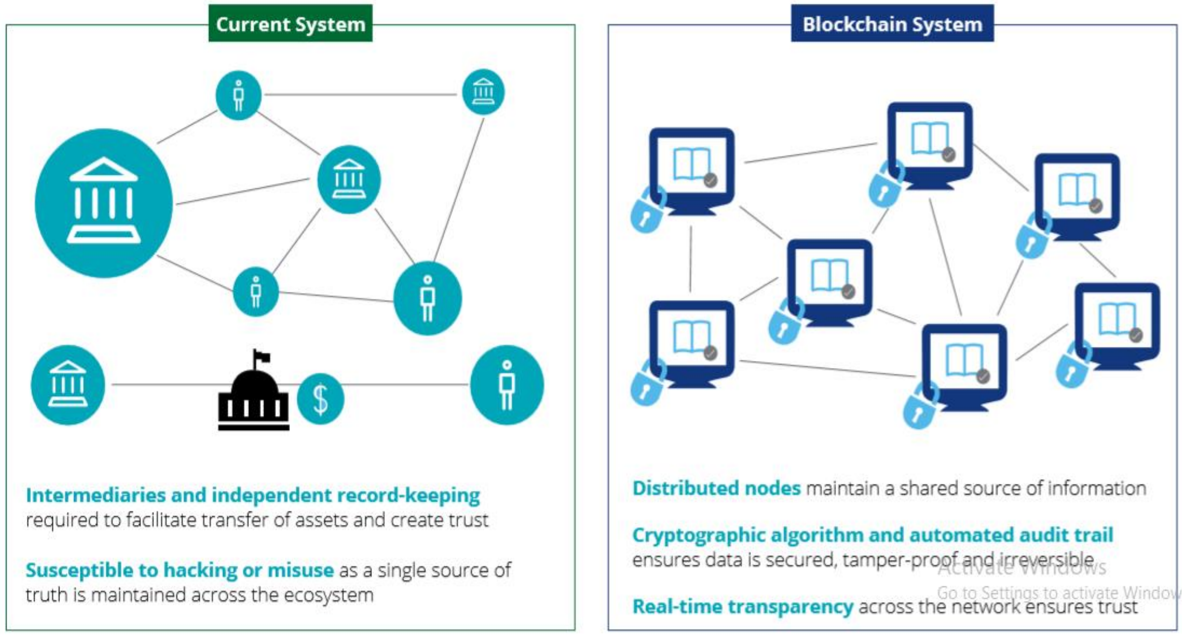
2.2.5 Blockchain in Public Sector – Deloitte

Organizations have traditionally recorded transactions in ledgers, kept under lock and key. Those ledgers are typically isolated to protect their accuracy and sanctity, and when conducting business, each organization maintains its separate record, to independently verify information (Berdik, *et al.*, 2021). In essence, blockchain is a ledger, but one with built-in trust. A blockchain is a digital, distributed transaction ledger, with identical copies maintained on multiple computer systems controlled by different entities. Anyone participating in a blockchain can review the entries in it but can update the blockchain only by consensus of a majority of participants. Once entered into a blockchain, information can never be erased; ideally, a blockchain contains an accurate and verifiable record of every transaction (Marthews, *et al.*, 2022).

Instead of relying on a third party, such as a financial institution, to mediate transactions, member nodes in a blockchain network use a consensus protocol to agree on ledger content, and cryptographic hashes and digital signatures to ensure the integrity of transactions (Stinner, & Tyrell, 2021). Blockchain, hence, offers several benefits such as reliability, data security, accuracy, and cost savings, etc. (refer to Figure 4).

Figure 3

Source (Deloitte analysis 2019)



2.2.6 A fit assessment framework for blockchain use cases

Today, governments, healthcare, and financial institutions are vigorously experimenting with multiple use cases of blockchain. While experimentation is necessary for a solution to emerge, it is important to select the right use cases for a better probability of a viable business case when the solution is scaled to production (Oluyisola, *et al.*, 2021). A blockchain-based solution is a good fit for use cases where multiple parties having low levels of trust, transact with each other. The technology is applicable in areas where the same transaction information is getting stored across disparate systems or databases. Blockchain fitment is also dependent on the time sensitivity of data, cost of reconciliation, need for data security, and requirement for authentication (Raj, *et al.*, 2018).

2.3 Design of Blockchain-Based Smart Contract Models

2.3.1 Blockchain technology

In the design of the tendering model, the study used Ethereum blockchain API, because Ethereum is an open-source platform that is publicly available and is a well-known choice for developing distributed applications. With Ethereum, each transaction had a 'gas' usage and 'gas cost' (Shi, *et al., 2022*). The 'gas' usage is determined by how computationally expensive the transaction is. The purpose of working out the 'gas' used in each transaction comes down to the fact that every node in the blockchain verifies the transaction.

The smart Contract which writes an Ethereum smart contract Solidity programming language is used. It is a general-purpose programming language that uses a class (*contract*) and methods that define it. Solidity's main purpose is to send and receive digital tokens as well as store states. Ethereum wallets which fully demonstrate the research objectives, we will create three types of wallets on Ethereum: for the bidder, for the tendering organization, and the contract respectively. Dapp is responsible front-end users will use Dapp to connect with the blockchain via the Smart Contract network (Front End → Smart Contract → Blockchain). The illustration on how the front-end users connect with the Dapp applications

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires consensus of the network majority (Lakhanpal, *et al.,* 2018). Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain (KAFOL et al., 2018).

Constantly growing as ‘completed’ blocks are recorded and added to it in chronological order, it allows market participants to keep track of digital currency transactions without central recordkeeping. Each node gets a copy of the blockchain, which is downloaded automatically. Within the blockchain is a block that is the ‘current’ part of a blockchain, which records some or all of the recent transactions (Ozercan, *et al,* 2018). Once completed, a block goes into the blockchain as a permanent database. Each time a block gets completed, a new one is generated. There are countless such blocks in the blockchain connected in chronological order. Every block contains a hash of the previous block.

A blockchain is a form of a distributed database. A distributed database is a collection of interrelated databases stored in multiple locations. In most traditional senses of the term, a distributed database is divided into portions that are then maintained in these separate locations. In the case of the blockchain, every participating node has a copy of the ‘database’ in its entirety (Hassija, et al, 2021). Meaning that the participating nodes do not need to trust each other to trust the data stored in the ledger. Each node can independently verify the data they are given and then decide to store that data in their copy of the database. This results in a database that grows by consensus. Transactions that are intended to be added to the blockchain are propagated through the network by the participating nodes. To mine a block, blockchains employ a consensus protocol that must be satisfied by the block (one such example is the proof-of-stake protocol). Once a block is mined, this new block is broadcast to the other nodes, which will then append it to their active chain (Akbar, et al, 2021).

These blocks will have a cryptographic hash in the header that relates to the previous block in the chain. Sometimes, two nodes will mine two different blocks at the same time, and both broadcast these blocks creates a fork in the chain. Nodes resolve this by always selecting the chain with the most work performed on it as their active chain. Resulting in the chain being supported by the majority of the nodes always becoming the active node (Wang, et al, 2021). Thus consensus of more than 50% of the nodes prevails. Ensuring the integrity of the chain, together with the consensus protocol and the cryptographic hashes. The general concept can only be spoken about vaguely because how this plays out in practice depends entirely on the implementation of the blockchain and the consensus protocol employed (Lohachab, et al, 2021).

2.3.2 Smart Contracts

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 does not rely on any trusted third party. Entities can agree with all of the terms transparent to them (Uriarte, et al, 2021). The same integrity checks that keep the transactions on the blockchain from being edited are also in effect here. This means that when entities agree, 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. 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 (Tern, 2021). With a Turing complete language, as is employed by Ethereum, smart contracts can be used to execute several functions. Therefore, smart contracts provide a trustless 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 (Lumineau, *et al.*, 2021); however though, “no viable smart contract systems have yet emerged. This is due to the lack of widespread use as well their legal status remain unclear (Wang, *et al.*, 2018).

Smart contracts are computerized transaction protocols that execute the terms of a contract (Hamledari, *et al.,* 2021). 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).

2.3.3 How Smart Contracts Work

A smart contract is a user-defined program running on top of a blockchain. Smart contracts allow the execution of credible transactions between mutually distrusting agents, without third parties. The major objective of smart contracts is to provide security that is superior to traditional contract law while reducing transaction costs (Lippmeier, *et al.,* 2019). Smart contracts have the following features:

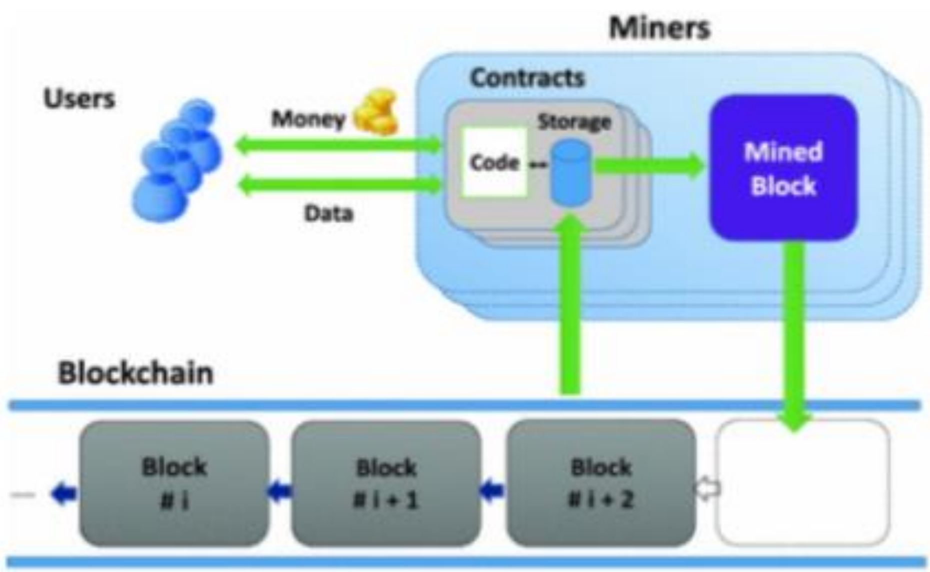
i. solely electronic nature
ii. software implementation
iii. increased certainty
iv. conditional nature
v. self-performance
vi. self-sufficiency

As illustrated in Figure 1, to deploy a smart contract in Ethereum, a special creation transaction is executed. This introduces a contract to the blockchain. During this procedure, the contract is assigned a unique address and its code is uploaded to the blockchain. Once successfully created, a smart contract is identified by a contract address. The Ethereum address identity is assigned to every individual participating in the transaction.

Each contract holds some amount of virtual coins and is associated with its predefined executable code. Cryptography plays a crucial role in this in that it is used for enforcement. The initiator of a transaction pays a fee (gas) for its execution, often measured in units of gas. Smart contracts automatically perform the contract terms according to the received information (Bergstra, et al., 2018).

Figure 4

The smart contract system (Lippmeier, et al., 2019).



The parties reach an agreement on the contents of the contract and perform the contracts according to the behaviors written in certain computer algorithms (Governatori, *et al.*, 2018). Smart contracts are self-executable and self-verifying agents that cannot be changed once deployed in the blockchain. Smart contract checks to see if participants in a transaction comply with the rules predefined in the smart contract. If they do, the transaction is validated; if not, the transaction is rejected. Smart contracts can be used to transfer assets of considerable value. Hence, their implementation must be secure and bug-free (Chatterjee, *et al.*, 2018).

2.3.4 Blocks

Blocks hold batches of valid transactions that are hashed and encoded into a Markle tree. (Meirobie, *et al.*, 2022) Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.

Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks (Maheboob, *et al.,* 2019). Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their database and retransmit the improvement to their peers. There is never a guarantee that any particular entry will remain in the best version of history forever.

Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks (Dotan, *et al.,* 2021). Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low. For example, bitcoin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. Several methods can be used to demonstrate a sufficient level of computation. Within a blockchain, the computation is carried out redundantly rather than in the traditional segregated and parallel manner (Zhu, *et al.*, 2021).

Block header, which is the metadata that helps verify the validity of a block. A typical block metadata contains version, previous block header hash, Time, and a Merkle root as shown in Table. 2 below;

Table 2

Visualization of block Metadata (Bathen, et al, 2018)

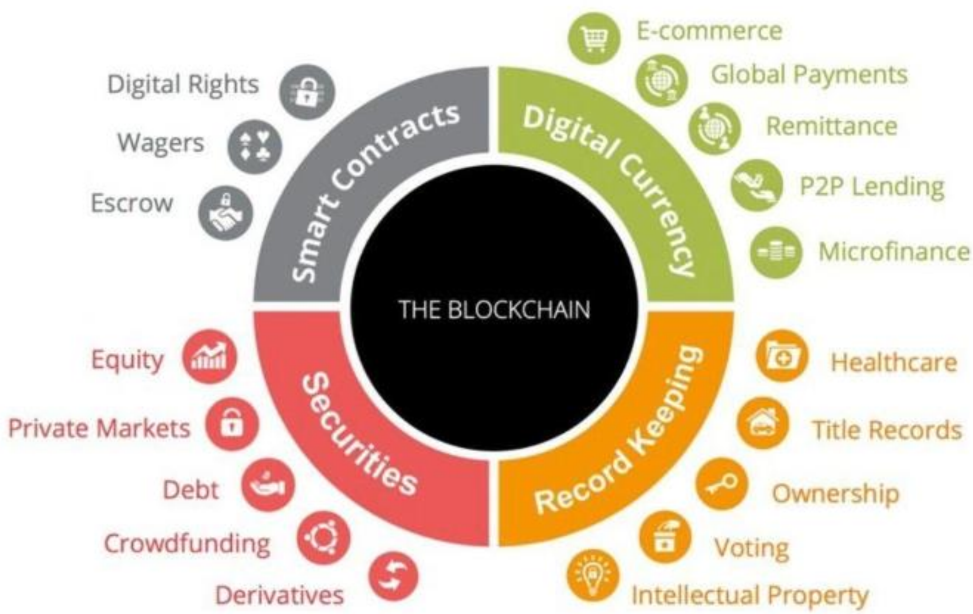
version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833

A block can be defined as a bunch of transactions that have been added to the blockchain. Blocks are a form of a data structure whose purpose is to bundle sets of transactions which are distributed to all nodes in the blockchain network. (Pradhan, 2022). In the Bitcoin, a block contains more than 500 transactions on average. The average size of a block seems to be 1MB. In Bitcoin Cash (a hard fork from the Bitcoin blockchain), the size of a block can go up to 8MB. This enables more transactions to be processed per second (Qiao, *et al.*, 2021).

The cool thing about blockchains is that they use cryptography to make sure that we notice it when any information on any page in the book is changed. This property makes it a good data structure to keep track of records of anything of value.

Figure 5

Blockchain's use cases (Qiao, et al., 2021).



2.3.5 The Validity of Blocks

When a miner solves the puzzle and mines the block, all the nodes in the network will check if the block is valid and add it to their copy of the chain. The nodes first need to reach a consensus on the validity. Only then does the network synchronizes and the state of the blockchain updates (Bhushan, *et al.*, 2021).

Nodes will only add a newly mined block to the chain if it follows the rules stated by the consensus mechanism. The software they run checks if a block is valid or not. An invalid block will simply be rejected (Dhurandher, *et al.*, 2021).

Naturally, a block is only as valid as the transactions contained therein. Using Bitcoin as an example, the rules of the protocol state that nobody can send bitcoins they have not first received from someone else or from mining a block. In other words, the nodes' software checks for all the transactions in a block if the senders have received enough Bitcoin to make their transactions (Zhang, *et al.*, 2021). To do this, they check the state of the network.

2.3.6 How Conflicts of Truth are Resolved

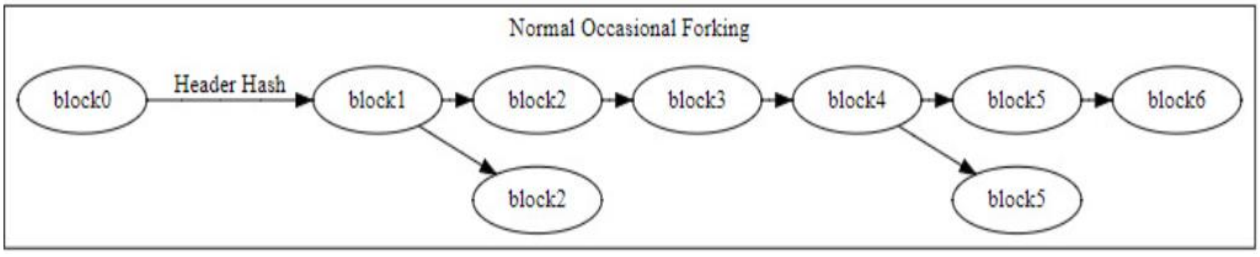
It can occur that, on accident, two miners add a valid block to the chain at the same time. Imagine that a part of the nodes has accepted one valid block and another part has accepted another block (Sompolinsky, *et al.*, 2021). The first group included a block with its transaction to Alice and the other included its transaction to Bob. Now we suddenly have two different states of the blockchain at the same time!

We call this an (unintentional) 'fork': The blockchain has forked in two different chains Does Alice or Bob have Bitcoin? Which of the two chains is the 'true' blockchain? (Sompolinsky, *et al.*, 2021).

Generally, all consensus protocols solve this problem with a simple rule: The longest chain wins.

Figure 6

Visualization of blockchain fork (Eyal, et al., 2016).



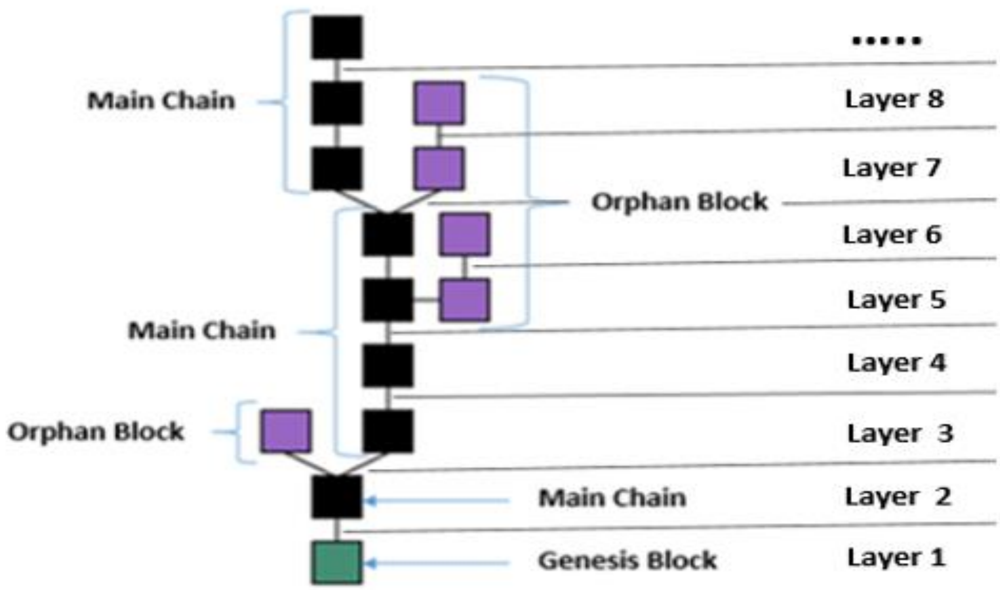
According (Sirer*, et al.,* 2018) when we have an unintentional fork, some miners will start mining on one chain, and others will start mining on another chain. Inevitably, one chain will have more miners than the other, and as such, will add new blocks to its chain faster. The rest of the miners will then switch over to the longer chain and the forked chain will always die out. No damage is done to the main chain.

2.3.7 Blockchain Formation.

The main chain consists of the longest series of blocks from the genesis block to the current block. Orphan blocks exist outside of the main chain as shown in fig. 8 below;

Figure 7

Blockchain formation (Khan, et al, 2018)



The very first block of all time, the "mother of all Blocks", is called the Genesis Block. Following a hierarchical arrangement, all blocks created afterward are organized in successive levels (or layers in the Blockchain jargon) corresponding to their time of creation. The newest Block is always on the top of the chain (Khan, *et al.*, 2018). Just like generations in a family tree, Blocks having the same parent Blocks are considered as "siblings" and lie on the same layer. Similar to human DNA, each individual Block possesses a unique identification code called a hash of a maximum of 80 characters.

Moreover, every Block also contains the ID of its predecessor in the same chain (Khan, *et al.*, 2018).

There is no limit on the number of Blocks that can be added to one chain: Blocks can be created infinitely and chains are continuously expanding vertically (John, *et al.*, 2021).

2.3.8 Block Time

The block time is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for Ethereum is set to between 14 and 15 seconds, while for bitcoin it is 10 minutes (Silva, *et al.*, 2020).

2.3.9 Hard Forks

A hard fork is a rule change such that the software validating according to the old rules will see the blocks produced according to the new rules as invalid (Yiu, 2021). In the case of a hard fork, all nodes meant to work following the new rules need to upgrade their software.

If one group of nodes continues to use the old software while the other nodes use the new software, a split can occur. For example, Ethereum has hard-forked to "make whole" the investors in DAO, which had been hacked by exploiting a vulnerability in its code. In this case, the fork resulted in a split creating Ethereum and Ethereum Classic chains. In 2014 the NXT community was asked to consider a hard fork that would have led to a rollback of the blockchain records to mitigate the effects of a theft of 50 million NXT from a major cryptocurrency exchange. The hard fork proposal was rejected, and some of the funds were recovered after negotiations and ransom payment (Gountia, & Satapathy 2020).

Alternatively, to prevent a permanent split, a majority of nodes using the new software may return to the old rules, as was the case of the bitcoin split on 12 March 2013 (Maheboob, *et al.*, 2019).

2.3.10 Role of Peer-to-Peer Networks

To use a blockchain as a ledger for transactional data, I have to be able to check in the blockchain if someone made a transaction to my address or wallet.

If the blockchain was only stored on one computer, and it happened to be turned off, this would be annoying, to say the least. Therefore, the current state of the blockchain is downloaded, synchronized, and made available by a large number of computers worldwide (Streitz, *et al.*, 2018).

These computers are called 'nodes', and they work together in a peer-to-peer network to ensure the blockchain is secure and up-to-date. Every one of these nodes stores the complete, updated version of the blockchain. Every time a new block is added, all the nodes update their blockchain (Thakur, *et al.*, 2020). Using a peer-to-peer network has certain advantages:

i. It can *always* check the state of the blockchain myself using a blockchain explorer.

ii. It doesn't have to rely on *one* party to know the true state of the blockchain.

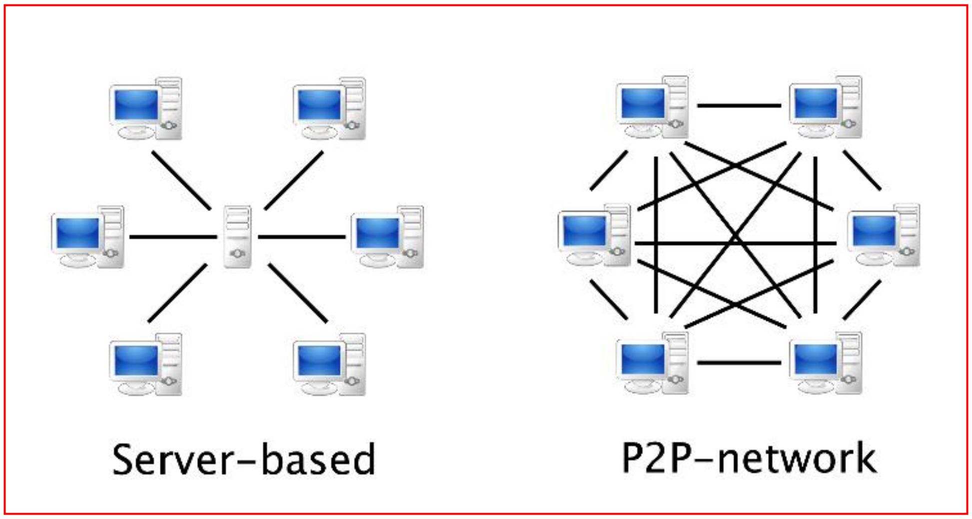
iii. It doesn't have to rely on the security of one server to know the blockchain is secure.

iv. A malicious party would have to hack thousands of computers at the same time, instead of one single server.

v. It can rest assured that the blockchain is never deleted because it would have to be deleted by all nodes.

Figure 8

A server-based model versus a peer-to-peer network (Thakur, et al., 2020).



This is all very important, but the above doesn't mean that the blockchain is now suddenly secure enough to be of any actual use to store or transact value.

For example, how do I know that the (transaction) data in the blockchain is correct? How do I know there are no invalid transactions in the blocks? And if there are different versions of the blockchain out there, how do I know which shows the true state of the blockchain?

These concerns are all taken care of, in a quite ingenious fashion, by the consensus mechanism, the use of which is made possible in the first place by the peer-to-peer network. Understanding the consensus mechanism, a peer-to-peer mechanism was used in '99 already by Napster. The blockchain, too, already existed before Bitcoin (Thakur, et al., 2020).

According to (Ducrée, 2022). Satoshi Nakamoto and the Origins of Bitcoin--Narratio in Nomine, the ingenious part of Satoshi Nakamoto's, the mysterious, anonymous founder of Bitcoin, white paper was combining the two with a consensus mechanism based on cryptography. The consensus mechanisms are where the real magic happens: it allows nodes in a peer-to-peer network to work together without having to know or trust each other (Coelho, et al., 2020).

The purpose of the consensus algorithm is to allow for the secure updating of a state according to some specific state transition rules, where the right to perform the state transitions is distributed among users who are given the right to collectively perform transitions through an algorithm.

In other words, a consensus mechanism is simply a set of rules, which is agreed upon by the nodes in the network by running the software of the network. These rules make sure the network works as intended and stays in sync (Jayabalan, & Jeyanthi 2021)

The consensus protocol sets rules on:

iii. How blocks are to be added to the chain.
iv. When blocks are considered to be valid.
v. How conflicts of truth are resolved.

2.3.11 Types of Blockchain

i. Public Blockchain

A public blockchain has absolutely no access restrictions. Anyone with an internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol). Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm (Kabbinale, *et all.,* 2018). Some of the largest, most known public blockchains are Bitcoin and Ethereum.

ii. Private Blockchain

A private blockchain is permissioned; one cannot join it unless invited by the network administrators. Participant and validator access is restricted.

This type of blockchain can be considered a middle-ground for companies that are interested in blockchain technology in general but are not comfortable with a level of control offered by public networks. Typically, they seek to incorporate blockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet (Singh, 2022).

iii. Consortium Blockchain

A consortium blockchain is often said to be semi-decentralized. It, too, is permissioned but instead of a single organization controlling it, several companies might each operate a node on such a network. The administrators of a consortium chain restrict users' reading rights as they see fit and only allow a limited set of trusted nodes to execute a consensus protocol (Chowdhury, *et all.,* 2020).

In consortium blockchain *consensus process* is controlled by a pre-selected set of nodes, for example, a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block for the block to be valid. The right to read the blockchain may be public or restricted to the participants. Some examples of consortium blockchains include R3 (banks) and EWF (Energy). Consortium blockchains are also referred to as federated blockchains. It has the following advantages:

i. Reduces transaction costs and data redundancies
ii. Replaces legacy systems, simplifying document handling, and getting rid of semi-manual compliance mechanisms.

2.3.12 Benefits of Blockchain

Blockchain is characterized by the following benefits;

i. Greater transparency

Transaction histories are becoming more transparent through the use of blockchain technology. Because blockchain is a type of distributed ledger, all network participants share the same documentation as opposed to individual copies. That shared version can only be updated through consensus, which means everyone must agree on it. To change a single transaction record would require the alteration of all subsequent records and the collusion of the entire network. Thus, data on a blockchain is more accurate, consistent, and transparent than when it is pushed through paper-heavy processes. It is also available to all participants who have permissioned access.

Enhanced Security

There are several ways blockchain is more secure than other record-keeping systems. Transactions must be agreed upon before they are recorded. After a transaction is approved, it is encrypted and linked to the previous transaction. This, along with the fact that information is stored across a network of computers instead of on a single server, makes it very difficult for hackers to compromise the transaction data.

ii. **Improved Traceability**

Any company that is dealing with products that are traded through a complex supply chain is usually known with how hard it can be to trace an item back to its origin. Therefore, using blockchain to record allows the creation of an audit trail that shows where an asset came from and every stop it made on its journey. This historical transaction data can help to verify the authenticity of assets and prevent fraud.

iii. **Increased efficiency and speed**

Compared with traditional paper-heavy processes where trading anything is a time-consuming process that is prone to human error and often requires third-party mediation, blockchain is known for streamlining and automating these processes, to yield transactions that can be completed faster and more efficiently. Since record-keeping is performed using a single digital ledger that is shared among participants, blockchain users don't have to reconcile multiple ledgers and they end up with less clutter (Xiaohan, & Yongqian, 2021). And when everyone has access to the same information, it becomes easier to trust each other without the need for numerous intermediaries. Thus, clearance and settlement can occur much quicker.

iv. **Reduced costs**

In most businesses organization, reducing costs is a priority. Using blockchain reduces the need for any third parties or middlemen to make guarantees because it doesn't matter if you can trust your trading partner. Instead, you just have to trust the data on the blockchain. It also won't have to review so much documentation to complete a trade because everyone will have permissioned access to a single, immutable version.

v. Decentralization

Instead of running a massive data center and verifying transactions through hubs, blockchain allows individual transactions to have their proof of validity and the authorization to enforce those constraints.

2.4 Research Gap

From the literature, it was noted that there is a gap in the existing models as illustrated on the table below;

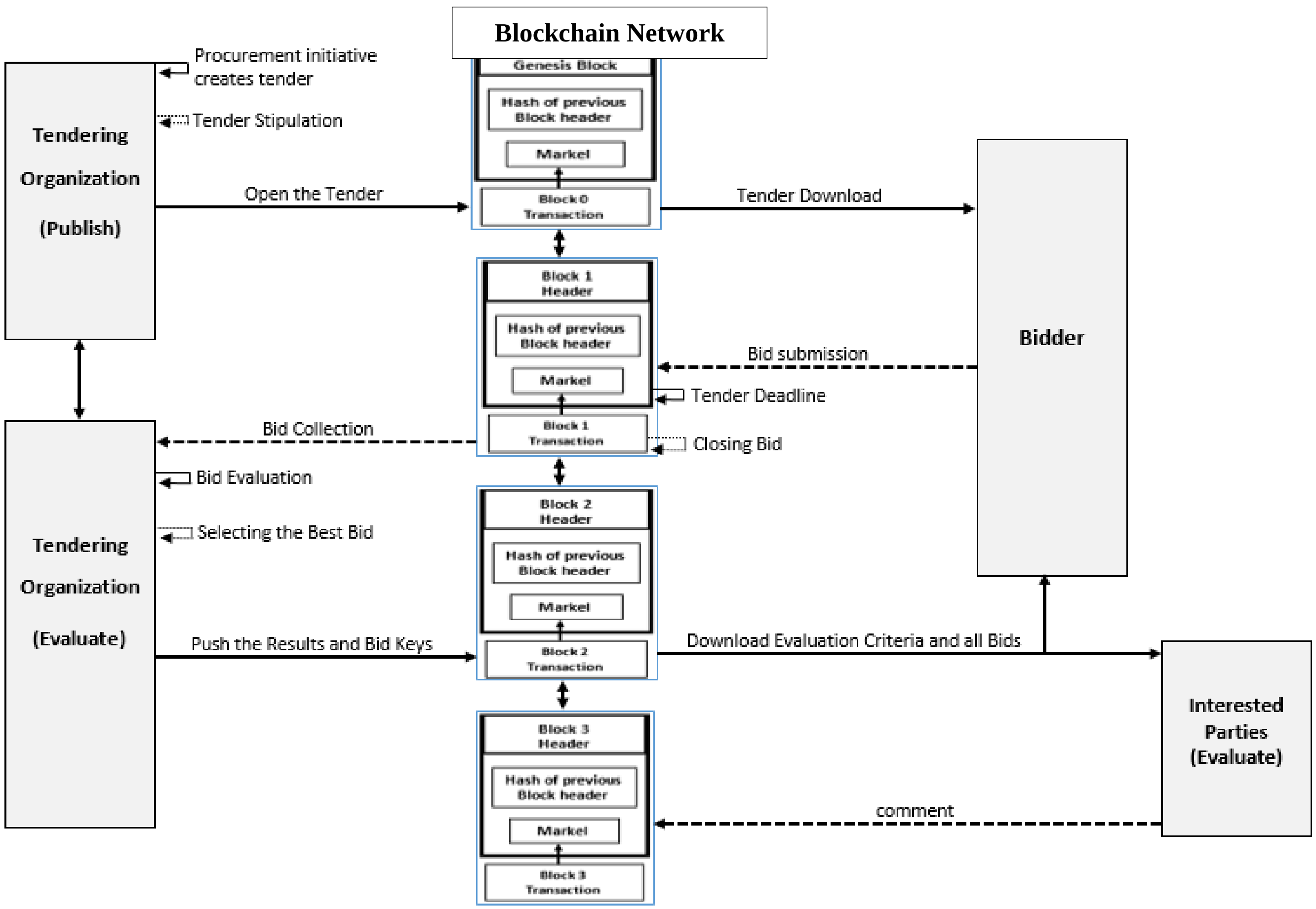
Table 2: Research Gap

Model	Strengths	Challenges
Web-based Tendering System (Palvia, *et al.*, 2007). Improved Internet-based technology to make it easy for tendering parties to interact and improve communications.	Focuses on ensuring anywhere anytime access of tendering adverts.	Issues about openness, transparency, Immutability, non-repudiation, and DB decentralization are not addressed.
E-Government Procurement systems (e-GP) (Neupane, *et al.*, 2014). The system allows electronic documents reviews, circulation, and tracking of procurement processes.	Focuses on the entire procurement process.	Openness, transparency, Immutability, non-repudiation, and DB decentralization are not addressed.
E-tendering system in Kenya – Focweb (Mutangili, 2019). The system facilitates the application of tenders online and provides a dynamic secure backend platform for the management and awarding of the tenders.	Reduce cost Reduces the transport cost of the bidder since they can bid online	Openness, transparency, Immutability, non-repudiation, and DB decentralization are not addressed.
E-Tendering System – ePPS (Nyaberi, 2020). Web-based, collaborative system to facilitate the full lifecycle of a tendering process, for both buyers and suppliers.	Online bid evaluation Creation and management of catalog-based information.	Issues about openness, transparency, Immutability, non-repudiation, and DB decentralization are not addressed.

2.14 Conceptual Framework of the Study

Figure 9

A conceptual framework (author 2019)



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 the bid evaluation code. A prospective bidder can download the tender from the blockchain. The respective bidder reviews the tender and considers the tendering specification and makes 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).

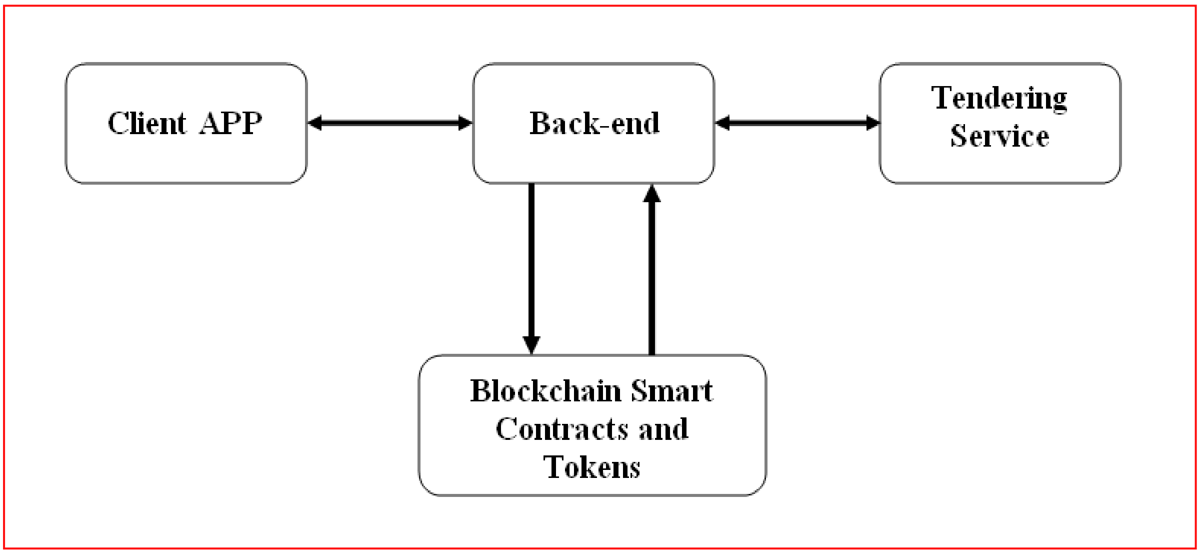
The symmetric key is then encrypted by the public key of tendering organization: (SKBidder). Half of the (SKBidder) is included as part of the submission and the second half would be communicated to the tendering organization at the tender submission deadline. The bidder will push the bid as a smart 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 registers 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, the 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 tender organization will push the results of the bid evaluations along with the 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)

2.15 Model Design and Operation

Figure 10

Model Design and Operation (Author 2019).



i. **Client APP-** A client application makes a call to the back-end API that is responsible for authorization and authentication. The request is then passed to the blockchain smart contract and a unique request ID is generated. After the successful tender initiation by the user, the backend receives the tender notification and sends it back to the smart contract for execution.

ii. **Account -** For a user to resolve his/her account, they send a request, and funds are transferred to the user's digital fiat currency account i.e. M-Pesa, and the user/ client tokens are transferred back to the smart contract.

iii. **Back-end -** This module allows the host or API to communicate with other applications such as the chain, smart contracts, and the connection to exchange. It is also concerned with tender creation, account creation, account deletion, tender execution, and tender transfer.

iv. **Smart contracts and token -** Responsible for a token generation and distribution to enhance miners are rewarded based on the running algorithm.

CHAPTER THREE

RESEARCH DESIGN METHODOLOGY

3.1 Introduction

This chapter discusses the methodology and research design followed in coming up with the Ethereum Based Solidity Smart Contract Model for tendering. The model was foremost designed and later implemented to provide a working prototype.

3.2 Objective Specific Research Design Methodology

A research design is a comprehensive outline of how research is conducted and involves the description of such considerations as obtaining data (Business dictionary, 2012). The specific methodologies followed in each of the research questions are discussed in sections 3.2.1 to 3.2.4 below.

3.2.1 Investigating Weakness in Existing Models

Given the above, this study employed a systematic literature review to answer research question one of the first objectives of the study. The results of these reviews allowed the study to establish the status of current knowledge on tendering models as shown in section 4.1.

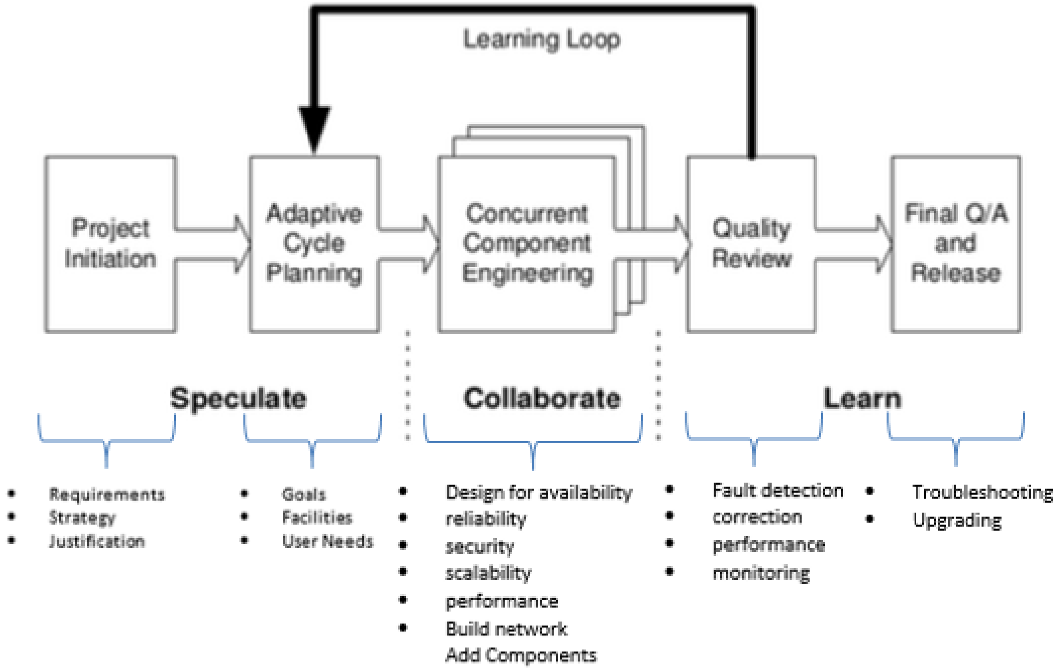
3.2.2 Design of the Blockchain Smart Contract Model for Tendering

To realize the Ethereum Based Solidity Smart Contract Model for Tendering Process, the Adaptive software development (ASD) process is used to create the experimental prototype as a proof of concept. The ASD leverages a repeating cycle of speculating, collaborating, and learning cycles. This dynamic cycle allows continuous learning and adaption to the emerging state of the model (Rotondo, & Quilligan, 2020). It is a life cycle dedicated to continuous learning and oriented to change, re-evaluation, peering into an uncertain future, and intense collaboration among researchers, supervisors, and any other evaluator (Recio-Saucedo, *et al.,* 2022).

The nature of the model is such that various components of the software would change and evolve thus a rapid and flexible development process which is the central principle of continuous adaptation. The figure below depicts the Agile Adaptive Software Development process.

Figure 112:

Model Development Methodology (Chua et al., 2003).



The prototype helped in creating a preliminary model of the idea and allow for quick testing and evaluation. By definition, a prototype is a model of something that is further realized in a commercial enterprise environment (Recio-Saucedo, *et al*., 2022). The model is in the form of a working web-based application to prove the feasibility of the Ethereum Based Solidity Smart Contract Model for tendering.

3.2.3 Model Development and Implementation

In the implementation of the tendering process, the study used Ethereum blockchain API, because Ethereum is an open-source platform that is publicly available and a well-known choice for developing distributed applications. With Ethereum, each transaction had a 'gas' usage and 'gas cost' (Kurt, *et al*., 2020). The 'gas' usage is determined by how computationally expensive the transaction is. The purpose of working out the 'gas' used in each transaction comes down to the fact that every node in the blockchain verifies the transaction.

If transactions were allowed to be arbitrarily complex, verification on the network would be slow and result in a processing bottleneck (Farahani, *et al*., 2021). Citing 'gas' needed for each transaction allows miners to determine whether or not it is worth including the transaction in the block that they are mining and they will use the cost of 'gas', as set on each transaction by the node that pushed it, to determine this. To mine one of these blocks, a node must satisfy the proof-of-work constraint (Ethereum's choice for the consensus protocol). This constraint necessitates a certain degree of work to be undergone by the node that wishes to push a block to the wider chain. This stops a node from pushing an arbitrary number of blocks to the chain: it would be computationally unfeasible (Li, *et al*., 2020).

i. **Truffle JS** - is used to create our contracts and write them in the Solidity language.
ii. **Private blockchain** -that runs on the TestRPC Ethereum client, is used for the unit tests during development.
iii. **Ropsten testing network** - Used for operational performance tests. This network most closely resemble the Ethereum production environment.
iv. **Infura.io node** – Used to connect to Ropsten.
v. **Blockchain explorer**- Used to interact with the contracts in **My Ether Wallet** using an account made via the **Meta Mask** chrome extension.

The model is categorized according to the subsection modules. The sections are organized according to achievable functions;

i. **The smart Contract -** To write an Ethereum smart contract, Solidity programming language is used. It is a general-purpose programming language that uses a class (*contract*) and methods that define it. The main purpose of solidity is to send and receive digital tokens as well as store states.

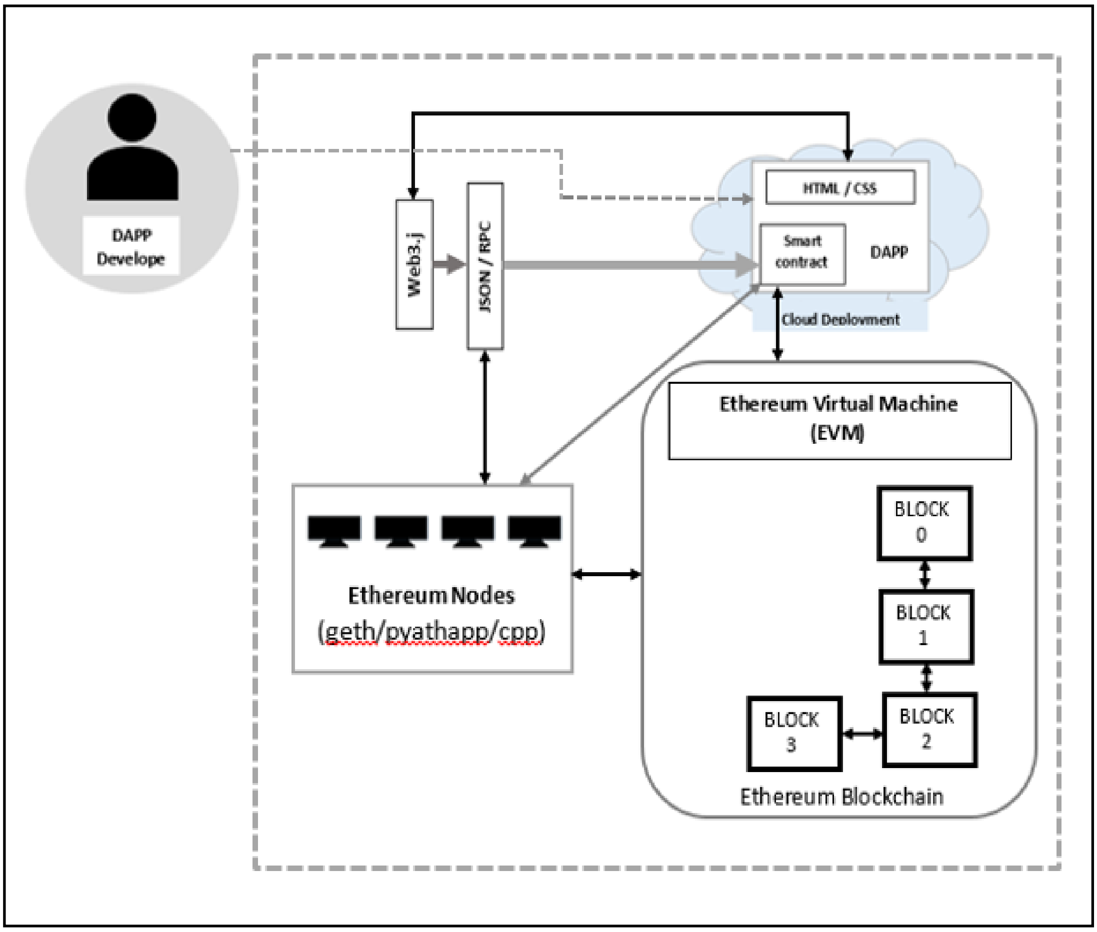
ii. **Ethereum wallets-** To fully demonstrate the research objectives, we will create three types of wallets on Ethereum: for the bidder, for the tendering organization, and the contract respectively.

iii. **Dapp** - The front-end users will use Dapp to connect with the blockchain via the Smart Contract network (Front End → Smart Contract → Blockchain).

The illustration on how the front-end users connect with the Dapp applications is shown below in figure 12.

Figure 123:

Model Development (author 2019)



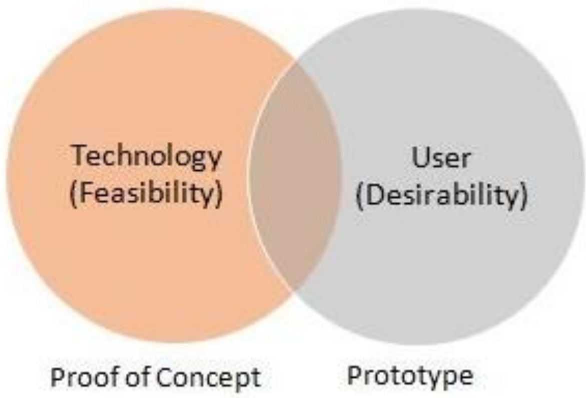
3.2.4 Model Testing and Validation

The proof of concept approach was adopted in validation and model testing. The study came up with an Ethereum Based Solidity Smart Contract Model for the tendering process. The potential technical and logistic issues required are identified in line with research questions (Kuperberg, *et al.*, 2019). The use of the proof of concept approach allowed demonstrating and verifying the practical potential of smart contracts in tendering (Ciotta, *et al.*, 2021).

This research aimed at building a model for tendering which provides non-repudiation, collision avoidance, confidentiality, and integrity – along with independent auditability features and evidential guarantees (Khan, *et al*., 2020). It has the potential to revolutionize the way organizations conduct their tendering activities, thereby achieving this research.

Figure 134

Integration of Technology and User experience created a Product (Takanen, et al., 2018).



The POC method adopted in this study allowed sharing internal knowledge among the tendering team and provided evidence of concept to the client for their product through a successful bidding process. First, POC research was conducted to prove that it's feasible to undertake successful procurement. Once this was proven, the POC was extended to develop an integrated working model to provide the snippet of the final product. Then it was later presented to the client and the product team to sell the idea for an upcoming project to be used internally within the development teams to share knowledge and stimulate innovation (Takanen, *et al.,* 2018).

3.3 Model Evaluation Technique

As pointed by (Davidson, 2018), the model evaluation approach is based on the idea that "the purposes, goals or targets" of the research is determined at the start and the evaluation process is used to establish whether the goals have been achieved and, if not, why not questions are used to amend missed functionalities. Goal-based evaluation as shown in section 4.3.2 was employed in model evaluation. Goal-based evaluation is a technical and economical evaluation approach whose main objective is to establish whether the prototype meets the set technical objectives (Fahmideh *et al,* 2018). Evaluating a system 'as such' is an evaluation approach that requires only the evaluator and does not involve the end-users (Vasarhelyi, & Halper, 2018).

3.3.1 Selection Criteria for Model Testing

Purposive sampling was adopted in selecting an organization to implement and test the suitability of the model. It is a form of nonprobability sampling whose main objective is to produce a sample that can be logically assumed to be representative of the population (Chakava, 2020). This is often accomplished by applying expert knowledge of the population to select in a nonrandom manner a sample of elements that represents a cross-section of the population. This sampling technique guaranteed only those organizations with viable Procurement and IT service.

This study obtained information from the Kenya Bureau of Standards (KEBS), a list of 15 organizations in Nakuru with certified processes. Among the organizations, two had existing e-procurement in place and therefore, they were selected for model testing. The list of the organization according to (KEBS, 2020) is attached in Appendix 5.

3.3.4 Ethical Consideration

During this research, several ethical considerations were put in place. Foremost, at data collection pre-visit, the researcher ensured that the information obtained from the technical staff about their existing e-procurement infrastructure was kept confidential. Further corroborating the confidentiality was the presentation of an introductory letter from the Institute of postgraduate and research of Kabarak University and a research permit obtained from the National Commission for Science Innovation and Technology (NACOSTI). The letters were presented beforehand upon a visit to the respective organization. Throughout the information gathering, exercise, and model development respondent's data was not misinterpreted or distorted in any form in model testing and reporting.

3.4 Summary

Openness and transparency are frequently discussed in the public service domain. Traditionally it has been difficult to build a transparent organizational model. This was because it required an investment of both time and money from all stakeholders. With the increasing adoption of new technologies, public opinion is in favor of developing innovative solutions that can increase openness and transparency in government activities with minimum cost to parties. For parties to be involved in monitoring the organization's activities, they need efficient tools and intuitive assessment that gives clear results. To build such an environment, blockchain and smart contracts show great potential which demonstrate that the tendering scheme can be made fully open, autonomous, fair, and transparent using smart contracts. To this end, it is successful.

CHAPTER FOUR

RESULTS AND DISCUSSIONS

4.1 Introduction

This chapter discusses the results of the study as per the research objectives. A report of existing tendering models, a prototype of blockchain-based smart contract implementation to assist tendering organization, and a report on the functionality of the Ethereum Based Solidity Smart Contract Prototype Model for tendering is presented.

4.2 Weaknesses of Existing E-tendering Models

To appreciate the importance of technology products, there needs to be a reason for the technology to exist. Therefore, to justify the need for a new blockchain smart contract model for tendering, the existing tendering models exhibit inefficiencies in their use case. The table below evaluates existing models and proposed models and clearly, there is a notable need for a blockchain model for tendering.

Table 3:

Existing Model Assessment

MODEL	OBJECTIVE	BENEFITS	CHALLENGES
Web-based Tendering System (Palvia, *et al.*, 2007).	Improved Internet-based technology to make it easy for tendering parties to interact and improve communications.	Focuses on ensuring anywhere anytime access of tendering adverts.	Issues about openness, transparency, Immutability, non-repudiation, and DB decentralization are not addressed.
E-Government Procurement systems (e-GP) (Neupane, *et al.*, 2014).	The system allows electronic documents reviews, circulation, and tracking of procurement processes.	Focuses on the entire procurement process.	Openness, transparency, Immutability, non-repudiation, and DB decentralization are not addressed.
E-tendering system in Kenya – Focweb (Mutangili, 2019).	The system facilitates the application of tenders online and provides a dynamic secure backend platform for the management and awarding of the tenders.	Reduce cost Reduces the transport cost of the bidder since they can bid online	Openness, transparency, Immutability, non-repudiation, and DB decentralization are not addressed.
E-Tendering System – ePPS (Nyaberi, 2020).	Web-based, collaborative system to facilitate the full lifecycle of a tendering process, for both buyers and suppliers.	Online bid evaluation Creation and management of catalog-based information.	Issues about openness, transparency, Immutability, non-repudiation, and DB decentralization are not addressed.

4.3 Design of Blockchain-based Smart Contract Model for Tendering

In the implementation of the tender model, Ethereum blockchain API has been used. This choice was made because Ethereum is an open-source platform that is publicly available and a well-known choice for developing distributed applications.

With Ethereum, each transaction will have a gas usage and gas cost. The gas usage is determined by how computationally expensive the transaction is. The purpose of working out the gas used in each transaction comes down to the fact that every node in the blockchain verifies the transaction. If transactions were allowed to be arbitrarily complex, verification on the network would be slow and result in a processing bottleneck. Citing gas needed for each transaction allows miners to determine whether or not it is worth including the transaction in the block that they are mining and they will use the cost of gas, as set on each transaction by the node that pushed it, to determine this. Trying to push a transaction that is too complex or with the gas cost set too low will cause a transaction to be ignored by the miners when they pick transactions to include in their block.

To mine one of these blocks, a node must satisfy the proof-of-work constraint, Ethereum's choice for the consensus protocol. This constraint necessitates a certain degree of work to be undergone by the node that wishes to push a block to the wider chain. This stops a node from pushing an arbitrary number of blocks to the chain, it would be computationally infeasible.

For a malicious node to corrupt a block halfway down the chain and present it as the valid active chain, it would also need to recompute every following block with its new cryptographic hash faster than every other participating node is working on their active chains.

TruffleJS framework is used to create contracts and write them in the Solidity language. For the unit tests during development, this study used a private blockchain running on the TestRPC Ethereum client, and the operational performance tests were done using the Ropsten testing network. To connect to Ropsten, the infura.io node is used. The blockchain explorer was used to interact with the contracts is MyEtherWallet using an account made via the MetaMask chrome extension.

4.3.1 Security and Operational Requirements

In this section, security and operation requirements are highlighted for implementation to satisfy the open and transparent tendering model:

i. The tendering Organization cannot change the tender once it is placed on the blockchain. If due to some unforeseeable reasons they have to change it, then they have to create a new tender (smart contract) on the blockchain.
ii. The tendering organization cannot read the bid until the deadline is expired.
iii. Bidders cannot change the bids of other organizations.
iv. Bidders cannot see who else has placed a bid.
v. Bidders cannot mount a Denial-of-Service (DOS) attack on their competitors to stop competitors from placing a bid on the blockchain.
vi. Blockchain networks or block miners cannot affect the tendering process.

4.3.2 Model Functional Overview

The implementation of this thesis is limited to four users: Administrator, bidder, evaluator, and common people. To describe the various functional requirement that users have on the application user functions are listed below. The different user types are thereafter defined in more detail in the table below.

Table 3

Model Functional Overview That Guides The Development Of The Model POC

Model Functionality	Function realization
1. Admin	The model ensured that Admin can cryptographically access tendering information, and no unauthorized entities can access it. It also ensured that Admin can set up and maintain accounts in the blockchain.
2. Tendering Organization	The bidding organization was able to verify the Bidder account & set a tender deadline. Also, they were able to see all the bids after the deadline and select the best bid & publish the results. Finally, the tendering organization was able to identify itself in a cryptographically secure manner upon accessing Organization's information on the blockchain.
3. Bidder	Was able to identify itself in a cryptographically secure manner upon accessing personal information on the blockchain and was able to see and update personal information upon registration. Also were able to view and create a proposal of the bid and submit it on the blockchain & check the account for bid results (ether wallet or token wallet).
4. Third Parties	Were able to create an account through registration on the blockchain and were able to view bid results.

4.3.2 User Overview and Interaction with Blockchain

The participating individuals in the blockchain-based smart contract model for tendering comprise of Admin, Bidder, Evaluator, third parties, and hosting service providers (EVM and MetaMask).

4.4 The Model Development and Implementation

Towards realizing the concept at a viable level of usability and security, the model was developed with web3 JSON RPC, metamask, ganache, truffle framework, node.JS, and geth client. Below is a user model functional overview.

First, create a bare Truffle project temple using Truffle commands, run them against an existing Truffle project. Once this operation is completed, a new directory for your Truffle project is created. Truffle requires that you have a running Ethereum client which supports the standard JSON, RPC, and API. MetaCoin box is used to create a token that can be transferred between accounts. When this process is done, you'll now have a project structure with the following items: Contracts directory for Solidity contracts, migrations directory for scriptable deployment files, test directory for test files for testing the application and contracts, and truffle.js for a truffle configuration file.

Each platform has an associated npm run configuration to help build on each platform. Because each platform has different (but similar) build processes, they require different configurations. To successfully demonstrate this transaction process the following steps were followed

Step I: Truffle with MetaMask Installation

For development with Truffle, this means dapp is used the same way users will interact with it on a live network. When interacting with smart contracts in a browser, make sure they are compiled, deployed, and interacting with them via **web3** in client-side JavaScript. The truffle-contract library is used, as it makes interacting with contracts easier and more robust.

MetaMask is the way to interact with dapps in a browser. It is an extension for a browser (Chrome or Firefox) that connects to an Ethereum network without running a full node on the browser's machine. It connects to the main Ethereum network, any of the testnets (Ropsten, Kovan, and Rinkeby), or a local blockchain such as the one created by Ganache or Truffle Develop. Once the MetaMask is installed, the front-end is ready to be used and to see the dapp running.

i. Using MetaMask with Ganache

Ganache is a graphical application that runs a blockchain that is used for testing purposes. It runs on **127.0.0.1** instead of **localhost** because the address does not require a network connection and is more suitable for development.

ii. Detecting MetaMasks's Web3 Injection

Before interacting with smart contracts in a browser, smart contracts are compiled, deployed via `web3` in client-side JavaScript using the truffle/contract library, while interacting with contracts is easier and more robust. Dapp is needed to check for MetaMask's **web3** instance and that the extension itself is configured properly with Ganache. MetaMask injects its **web3** instance after the window has loaded, the following checks are performed:

Table 4

Injected Web3 Instance

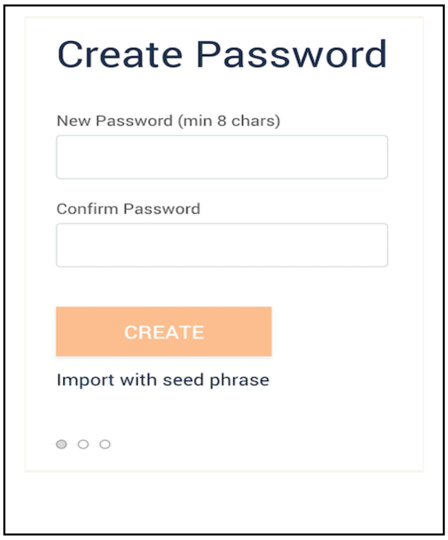
```
// Is there is an injected web3 instance?
if (typeof web3 !== 'undefined') {
  App.web3Provider = web3.currentProvider;
  web3 = new Web3(web3.currentProvider);
} else {
  // If no injected web3 instance is detected, fallback to Ganache.
  App.web3Provider = new web3.providers.HttpProvider('http://127.0.0.1:7545');
  web3 = new Web3(App.web3Provider);
}
```

iii. Setting up MetaMask

To use Ganache with MetaMask, the MetaMask icon in your browser is selected and this screen will appear:

Figure 145

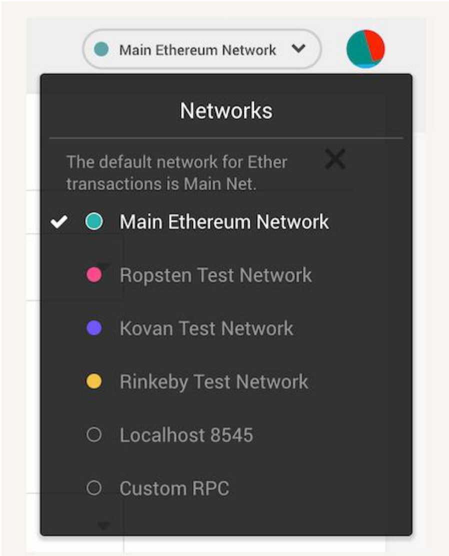
Metamask Initial Screen



MetaMask is then connected to the blockchain created by Ganache. At the menu that shows "Main Network", **Custom RPC** is selected.

Figure 156

Metamask Network Menu



Once MetaMask is connected to Ganache, it is taken to the accounts screen. Each account created by Ganache is given 100 ether. The first account should have less than the others because that account supplies the gas for smart contract deployment. Since you've deployed your smart contract to the network, this account paid for it.

iv. Using MetaMask with Truffle

Truffle Develop is a command-line application that runs a temporary blockchain that is also used for testing purposes. It runs on **127.0.0.1:9545**.

Using MetaMask with Truffle Develop is very similar to that of Ganache. The only difference is that Truffle Develop runs by default on **127.0.0.1:9545**, so the web3 code is edited as below.

Table 5

Metamask With Truffle

```
  // Is there is an injected web3 instance?
if (typeof web3 !== 'undefined') {
  App.web3Provider = web3.currentProvider;
  web3 = new Web3(web3.currentProvider);
} else {
  // If no injected web3 instance is detected, fallback to Truffle Develop.
  App.web3Provider = new web3.providers.HttpProvider('http://127.0.0.1:9545');
  web3 = new Web3(App.web3Provider);
}
```

Step II: Geth Client

Geth is the program that communicates with the Ethereum Network and acts as the relay between your computer, its hardware, and the rest of the ethereum network computers so if a block is mined by another computer your Geth program will pick it up and then pass on the new information onto your GPU or CPU for mining. Geth is the command-line interface for running a full ethereum node implemented in Go.

By installing and running geth, you can take part in the ethereum frontier live network and

i. mine real ether
ii. transfer funds between addresses
iii. create contracts and send transactions
iv. explore block history

JavaScript Console: geth can be launched with an interactive console that provides a JavaScript runtime environment exposing a JavaScript API to interact with your node. JavaScript Console API includes the web3 JavaScript Dapp API as well as an additional admin API. JSON-RPC server: geth can be launched with a json-rpc server that exposes the JSON-RPC API.

Step III: NodeJS

Node.js is an open-source, cross-platform, JavaScript run-time environment that executes JavaScript code outside of a browser. Node.js lets developers use JavaScript to write command-line tools and for server-side scripting - running scripts server-side to produce dynamic web page content before the page is sent to the user's web browser. Consequently, Node.js represents a "JavaScript everywhere", unifying web application development around a single programming language.

4.4.1 Development of the Tender Process Module

Process I: Initiating a Tender

The Request for Tender (Process 1) is initiated by a contract placed on the blockchain. This contract is created with a length, given in milliseconds, that determines how long the contractors (also referred to as Tendering Organization: TO) have to place their bids. This time is calculated using the Unix Epoch time at the time of creation. An upper limit is also given, which is used to control the number of tenders a contractor can place for this auction. The entity that created the auction is also required to pass in a public key that is specific to this request for a tender contract. These three attributes are held in the contract’s state.

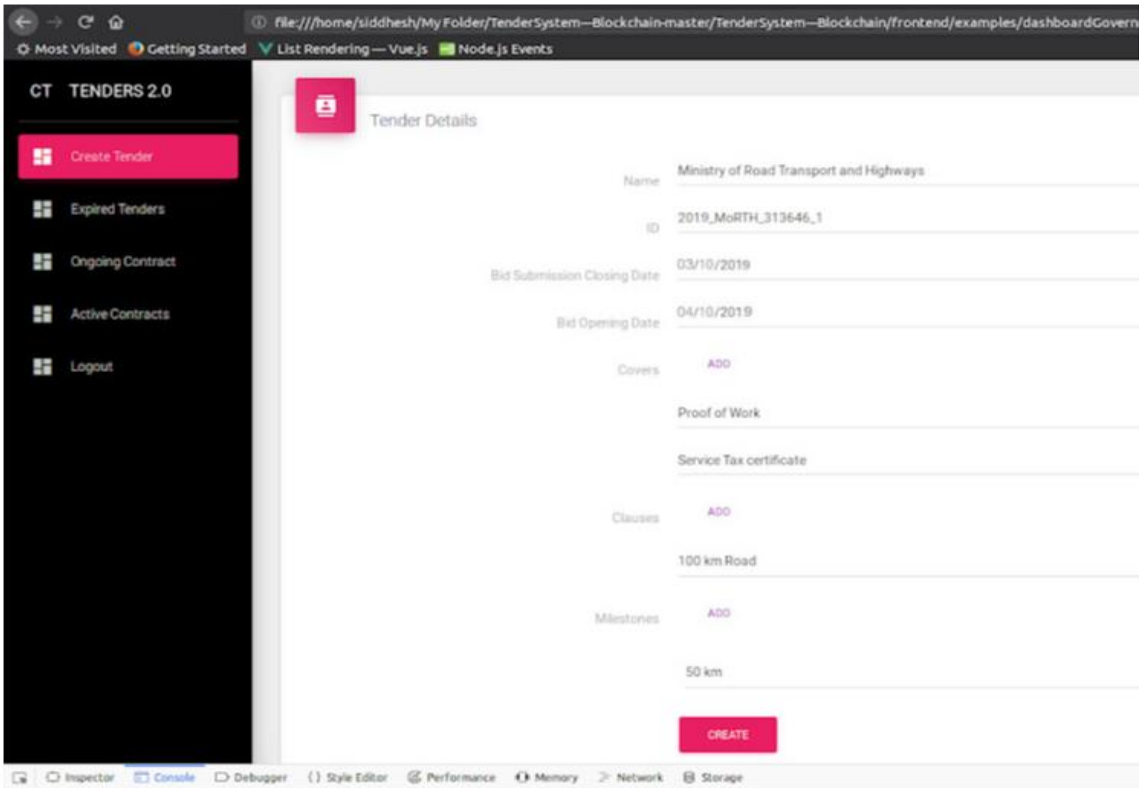
Table 6

Initiating a Tender

```
procedure REQFORTENDER(_length,_pubk,_limit)
biddingEnd ← TimeNow() +_length
limit ← limit
pubk ← pubk
```

Figure 167

Initializing a Tender



Process II: Placing a Bid

When a contractor places a tender (Process 2), the first step is to place a smart contract elsewhere on the blockchain that contains only the tender data. Experiments on the Ropsten test blockchain showed that 5000 bits could be stored on the blockchain with a gas consumption that didn't get immediately rejected for being too expensive. This roughly translates to 700 words. This study suggested that usually more verbose tender contracts are adapted for this format, perhaps by extracting the key information (PTO) necessary for the tender. The data on this contract is available to anyone maintaining the blockchain, and so is protected through the encryption performed using the bidders' bid-specific symmetric key sealed by PTO (SKBidder).

Placing the tender for the auction involves using the auction smart contract. The contractor passes in their ID, which should have been pre-agreed between the auction creator and the contractor, the address of their tender data on the blockchain, and then the components of the certificate that will have been given to them by the auction creator. This certificate should be signed using the private key that corresponds to the request for tender's public key that is put into the contract upon creation. To offload some of the computational complexity of the contract, the parts of this certificate which are then hashed message, and the v, r, and s values are extracted on the client-side. The request for tender will take the address of all placed tenders and store it in an array.

All tenders left on the contract are recorded, but the validity is determined using the certificate, the time that the tender was placed, and the record of bids placed. The time when the tender was placed is retrieved using the now () function available on an Ethereum contract. The now () function uses the time from the epoch registered on the node executing the transaction.

This timing can be considered trusted because of the timing consensus of nodes on the blockchain. Nodes are unable to mine blocks that have timestamps earlier than the parent blocks time stamp. Nodes are discouraged from placing blocks at an arbitrary amount of time ahead for the same principle, few nodes on the chain are willing to put a block on the chain far ahead of their current time because it is unable to place new blocks on top of it, thus stopping the block from getting picked up by a majority of nodes. Nodes are also discouraged from moving the time back because the challenge issued in the proof-of-work is orders of magnitude

Figure 178

Placing a Bid

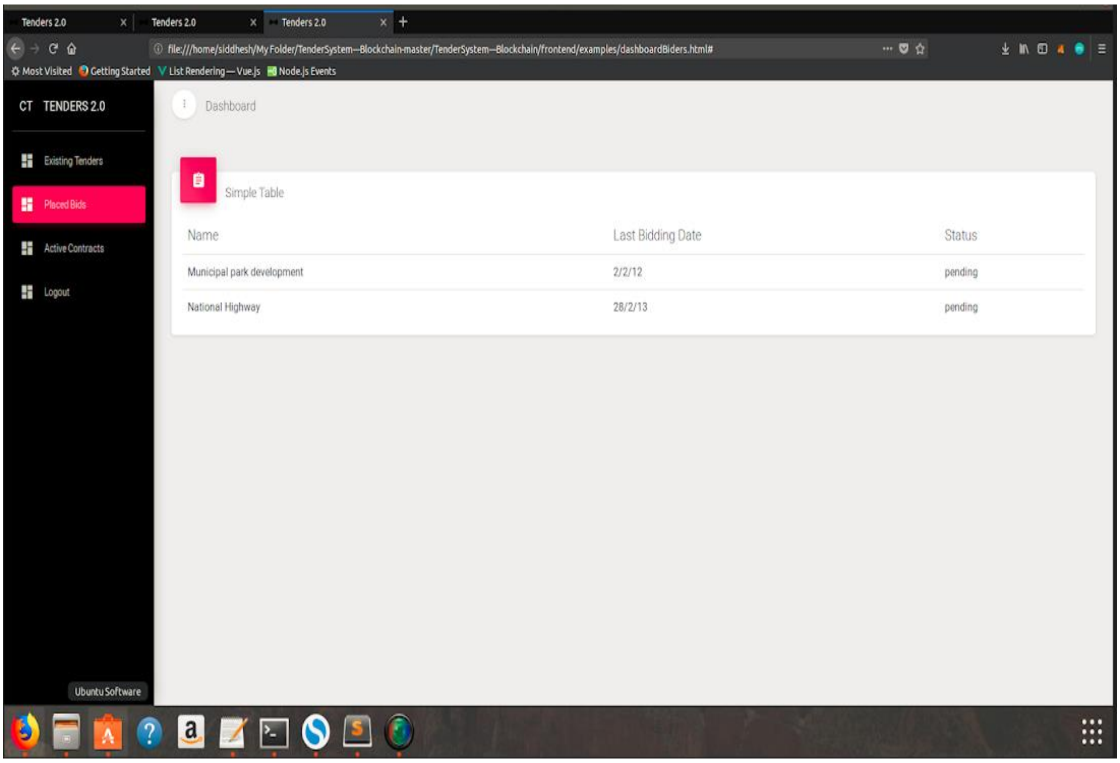


Table 7

Placing a Bid

```
procedure PLACEBID(id,data,msgHashed,v,r,s,)
bidV alidity ← V alidBid(id,msgHashed,v,r,s)
if bidV alidity then
bidCount[id]+ = 1
bid←newBid (id,data,bidValidity,bidsPlaced,biddingEnd)
bidsPlaced.add(bid)
return bid
procedure VALIDBID(id,msgHashed,v,r,s,)
validHash ← verify(msgHash,v,r,s)
validTime ← timeNow() < biddingEnd
allowedBid ← bidCount[id] < limit
return validHash and validTime and allowedBid
procedure BID(_id,_data,_validity,_bidsPlaced,_biddingEnd)
id ←_id
data ←_data
validity ←_validity
bidsPlaced ←_bidsPlaced
biddingEnds ←_biddingEnd
```

A bid is considered valid if the following hold;

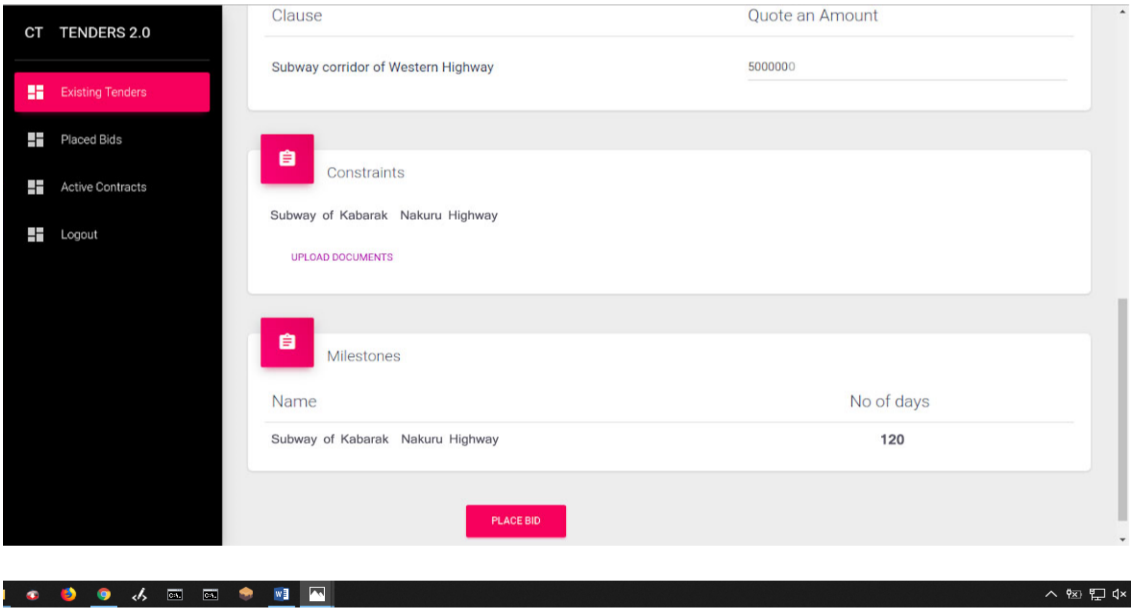
i. The contract is placed within the time
ii. The certificate is verified to match the public key held by request for tender contract
iii. The contractor is allowed to place more bids.

If it fails any of these checks, it is still placed but flagged as an invalid bid. The number of bids placed by the contractor is only incremented if it is being placed using a valid certificate, protecting the contractor from being locked out of the auction by a malicious party placing arbitrary numbers of bids using their identifier.

The tender reference smart contract is then created and passed the id of the contractor, the address of the tender data, the validity of the contract, a copy of the array holding all of the addresses of the tenders placed before this one, and the auction end time. The address table is required to ensure the integrity of the array revealed by the auction creator – no bids could be intentionally erased from the array because the record of its existence will exist in the tender reference contracts.

Figure 189

Bid Verification



Once the auction time has elapsed, the addresses can be requested from both the request for the tender contract and the tender reference contracts. Process 2 performance indicates that altering the contract's state to hold the addresses increases the gas usage, and thus the cost, on each subsequent transaction.

Process III: Bid Evaluation

Process 3 is a retrieval algorithm that is only applicable to the schemas where the addresses are held in the state of the Request for Tender contract. The addresses would be retrieved from the contract after the request for the tender period has elapsed. The client application is used to interact with the blockchain will request the contract on the blockchain. Retrieving the information does not require any transactions and thus incurs no transaction cost.

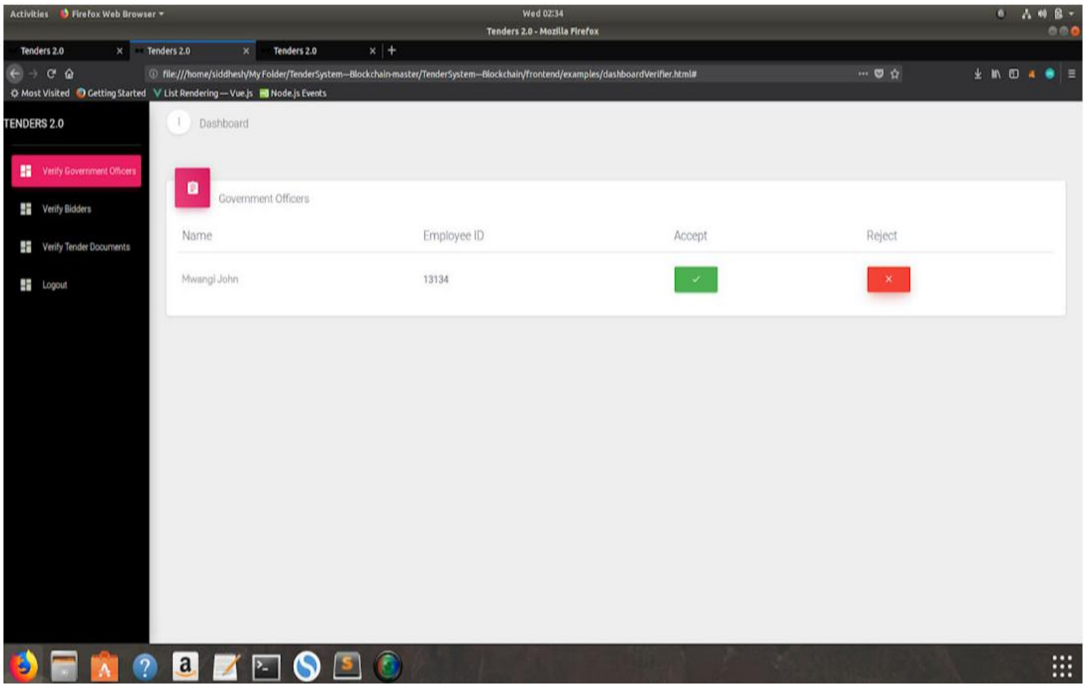
Table 8

Bid Evaluation

1: procedure MAKEREQUEST(_length,_pubk,_limit).
2: listOfBids ← ReqBids()
3: for bids in listOfBids do
4: validBid ←bids.getValidity()
5: if validBid then
6: listOfValidBidDataAddresses.add(validBid.getDataAddress())
7: procedure REQBIDS(length, pubk, limit) . Running in the blockchain

Figure 19

Bid Evaluation



The client application will receive a list of bids which is the addresses of the bids placed. These bids can then be queried for their validity and, once ascertained, the address of the actual tender data can be requested.

4.5 Model Prototype Validation and Verification

The tendering organization PoC fulfills all the goals, inspiration for how each of the goals is satisfied is exposed in Table 12 and blockchain attributes in Table 13. For details on the code, the reader is directed to Appendix I where the full source code can be found. Besides the functional criteria, additional requirements were defined to cover non-functional aspects of the PoC. These are evaluated in goal based on the theory seen in Chapter 2 of this thesis.

The prototype presented in section 4.3 was evaluated and verified to ascertain how the model overcomes the weaknesses of the existing models based on the two organizations that interacted with the blockchain tendering model. For details on the sample report by the two testing organizations, the reader is directed to Appendix VI and VII.

Table 9

Evaluation of Goals Based On Tendering Blockchain Model: (Researcher, 2019)

Goal	Evaluation Results
1. **Admin:** The goal was to ensure Admin identifies to the blockchain cryptographically and securely upon accessing the tendering information	The prototype succeeded in capturing Admin details upon registration on the blockchain. Also, the log details were able to be captured and protected using an encryption scheme for security.
2. Tendering organization: The user should be able to create an account and access the Organization's information in a cryptographically secure manner. Also be able to create, open a tender for bidding and verify the Bidder account & set a tender deadline. The user should see all bids after the deadline and select the best bid & publish the results.	The user was able to create an account and additionally access organizations' information securely. In addition, the bidding organization was able to cryptographically open the tender for bidding and set a tender dateline. The tendering organization was able to see all the bids after the deadline for evaluation and subsequently publish the results on the blockchain.
3. Bidder: Identify myself in a cryptographically secure manner upon accessing my personal information on the blockchain and be able to see and update my personal information upon registration. Also, be able to view and create a proposal of a bid and submit it on the Blockchain.	The bidder was able to identify himself and access the bid has presented by the bidding organization. Also was able to create a bid proposal and submit it on the blockchain for evaluation by the tendering organization. The bidder was able to check the results on his account after the evaluation of the tender.
4. Third parties: Be able to create an account through registration on the blockchain and be able to view bid results.	The external third parties were also able to login and view the smart contract facilities including bid results for closed tenders

Table 10

Evaluation of Attributes Based On Tendering Blockchain: (Researcher, 2019)

Attributes	**Evaluation Results**
Accessibility	The model ensured that all users are registered before allowing them to access any of the model functions. The registered persons can log in using their account addresses and passwords.
Usability	Anytime a binding contract is terminated, the bidder details are removed from an active account to a repository. Also, the model enables authorized users to generate reports regarding transactions.
Reliability	Every node on the blockchain network has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it is valid, then it is added to the ledger. This promotes transparency and makes it reliable
Security	The model gets rid of the need for a central authority, no one can just simply change any characteristics of the network for their benefit. Using encryption ensures another layer of security for the model.
Decentralization	The model did not have any governing authority or a single person looking after the blockchain network. Rather a group of nodes maintains the network making it decentralized.

4.5.1 Organization Specific Report on Model Testing

Upon passing of the procurement and disposal act 2015 by the government of Kenya. It is a requirement for both private and public organizations to comply with ISO 9001 processes. 15 registered Organizations in Nakuru had been mapped by KEBS to have complied with the above-mentioned regulations at the time of this research. Of those organizations, two were using IT-based procurement tendering services. Therefore, this research used the two organizations in the model testing. They were allowed to interact with the blockchain tendering model and the report is presented from samples Organization A and B as shown below.

i. Organization A Sample Report

As shown in the table below, it can be noticed that Organization A registered 6 bidders into the platform and all of them submitted their bids using ETokens equal to the value of their item quotation. The blocks of transactions can be trailed from when the bidding organization opened the dander for bidding to start. Other transactions captured including registration, signing agreements, and information updates are captured in the blockchain.

Table 11

Organization a Sample Report

TX hash	Block no	Timestamp	Date Time	From	To	Quantity
0xa4df7c7bd246a9e5de7bfd6bac29e9a5cadffa 3a6da2dd8ac4a22faeced772ca	5102742	1551259083	6/29/2021 11:00	0xc6e532bb14d444a4af146 14f300453609018c96c	0x32cd37a01a628605850 7d1f018c8cb8676a90aaf	3000
0x8f2a22c99ab613f27201062f08c82 51ba2669a3dd5dd83e5119bd7dd41559479	5137983	1551718836	6/29/2021 11:05	0x0289bd742d56e94dd04f7b a09185c5a139b35b2f	0x32cd37a01a6286058507 d1f018c8cb8676a90aaf	2300
0x315d74a791457efec5c9a176a30e 983f4f3d15176064de335648a806f0f03316	5234443	1552992765	6/29/2021 11:30	0x13e7b6833e25e19b9d19ba 3153bb95c173afdd34	0x32cd37a01a6286058507 d1f018c8cb8676a90aaf	1700
0xdd787bd3a83f166289fcd3b4 b91b8e02e9fa2e0d2895b36e5b93336ace5b02a1	5235275	1553003197	6/30/2021 10:10	0x13e7b6833e25e19b9d19 ba3153bb95c173afdd34	0x32cd37a01a6286058507 d1f018c8cb8676a90aaf	1100
0xa799b13f9150e48c8bf8c85e09c0ee d0a72c85ee0b8243865ed1d1dcefbd5217	5235278	1553003214	6/30/2021 10:12	0x13e7b6833e25e19b9d19b a3153bb95c173afdd34	0x32cd37a01a628605850 7d1f018c8cb8676a90aaf	2000
0x4e4b945584bb863b3a648b70e00 7130db4f214294f72fe2f8d39322f94c979b2	5235449	1553005518	6/30/2021 10:15	0x13e7b6833e25e19b9d19b a3153bb95c173afdd34	0x32cd37a01a628605850 7d1f018c8cb8676a90aaf	2760
0x693fe0148757bdc6977d728a871 1b8ec8814fc6e9593a343681c55a67bf69ac6	5710843	1559395986	6/30/2021 10:16	0xebd3872ea4d1d85a03a58 1127b872c99ebbab000	0x32cd37a01a628605850 7d1f018c8cb8676a90aaf	1900

ii. Organization “B” Sample Report

As shown in the table below, it can be noticed that Organization B registered 11 bidders into the platform and all of them submitted their bids using ETokens equal to the value of their item quotation. The blocks of transactions can be trailed from when the bidding organization opened the dander for bidding to start. Other transactions captured including registration, signing agreements, information update, or removal are captured in the blockchain.

Table 12

Organization a Sample Report

TX hash	Block no	Timestamp	Date Time	From	To	Quantity
0x718d928d0fd11e0aa208f68790fd6cc5fae209d02f94 8e7d28ee34b30c9ddd37	5710830	1550747144	7/2/2021 10:12	0x236ad9817ae3d957532e279469 eb86f1dd673d8	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0xde802d9d1551c1034a33229de120b7ec8f439b09ff3 4532321fff6e34c6dbb62	5710830	1550747180	7/2/2021 10:13	0x08e743af812a37751c1cfc0fd61 f6b997eec0c6c	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0x22762b88615c52f8fc00b19bbd8edbf4d1ccfb4ba2a1 a32bf2301c6b0ad8a35b	5710830	1550747237	7/2/2021 10:15	0x64404296855fef130c1f215a3db f9d940b332607	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0xca5532d2db4b4c52a0167172e2762dd2a3a0e37b9d8 1131397229e83d8258244	5710830	1550747399	7/2/2021 10:20	0x3f4eb593904495a346df4bc7c80 a55a519aa4295	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0x493dd0186d383d43c515b2a752b2ea16d88c446bf91 0070610a1792bb9825b07	5710830	1550747710	7/5/2021 12:04	0x3f4eb593904495a346df4bc7c80 a55a519aa4295	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0x5241679488b904366221c183f26aa531e6129e0a047 e479037f26b4f612e10ec	5710830	1550748107	7/5/2021 12:10	0x08e743af812a37751c1cfc0fd61 f6b997eec0c6c	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0xf849bdc366a4a85700f703b541ef323d15b4c450b43 e4d0766dbc510429916	5710830	1550748160	7/5/2021 12:11	0xcc2acae48f60a324c8ae0fa2c99 1b8e741d72652	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0xbfdede075bdf7966d01952e0a0c55dedc7e030b4b60 c332e8494eaf230339097	5710830	1550748166	7/7/2021 11:24	0x13e7b6833e25e19d19ba3153bb 95c173afdd34	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0x34b7190f2f17db1057ae3c1b8aa35c6d0db804043c3 76a5c14efb60235705d76	5710830	1550748223	7/7/2021 11:30	0xbb84b6d71c6c662609bc1b971c 9a1d9b2eb5000	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0xe9c2d81af3a12f6a76ac798ef19f92be377d21229375 c479849a3c121c26dccc	5710830	1550748308	7/7/2021 11:32	0xfe96912711c1fc37168df6e84e0 290339f3b2141	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000
0x2ddabe39c7479e4b988f51231dfbecfa59e3e840606d b0a3aeb797348d9c74e5	5710830	1550838175	7/7/2021 11:40	0x69670b0c1b10073812415dd474 804bb32b3aeca	0x13e7b6833e25e19b9d19ba3 153bb95c173afd	5000

The above test data, from the two organizations, shows blockchain consisting of a series of blocks that are used to store information related to transactions that occur on a blockchain network. A block (row) contains a unique header, and each such block is identified by its block TX hash (transaction hash) and other information /blockchain parameters as discussed in section 2.3. Though not all the block header or body information is represented here, it can adequately prove blockchain transactions. Based on the assessment criteria presented in Table 13 (Key of Assessment Criteria), the following describes the fulfillment of these criteria.

a) Transparency

Fulfilled by blockchain infrastructure both in the component and the contract layer where transactions are recorded in a distributed ledger thus improving Transparency. Public verifiability allows anyone to verify the correct system working. This also ensures a situation in which transaction activities are done openly without the need for a trusted party. The following figure presents a Block Explorer that allows users to easily lookup, confirm and validate transactions that have taken place on the Ethereum Blockchain. This promotes transparency and transaction verifiability.

Figure 201

Blockchain transparency

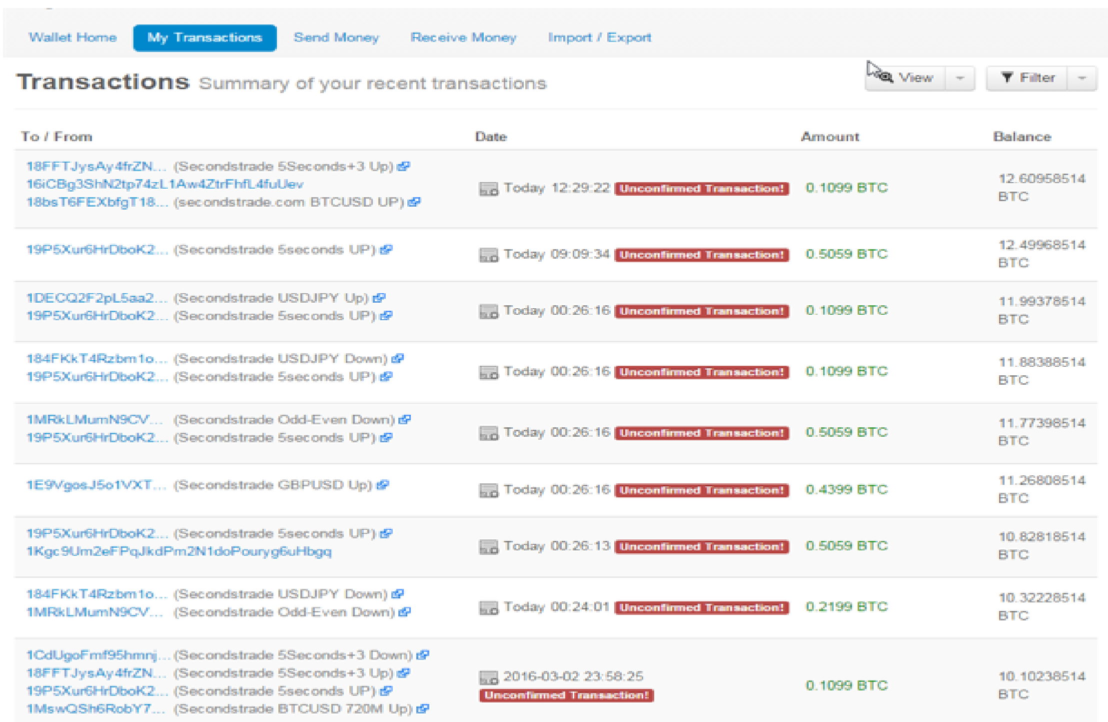
Txn Hash	Block ↓	Mined On	From	To
0x96f7a818...1e364	13421974	2021-10-15 12:00:23 PM	0x1318fbc9...1637d	0x5c69bee7...5aa6f
0x014ed80f...3393b	13421973	2021-10-15 11:59:06 AM	0x188408ef...02348	0x0210788b...b6496
0x0512f236...63fa6	13421973	2021-10-15 11:59:06 AM	0x1938a448...45ad0	0x40d60260...be121
0x0536da99...32523	13421973	2021-10-15 11:59:06 AM	0x1938a448...45ad0	0xb64ef51c...ab8ac
0x06252b1c...7992e	13421973	2021-10-15 11:59:06 AM	0x1938a448...45ad0	0xfe756b3d...788ce
0x069a32c5...b3d04	13421973	2021-10-15 11:59:06 AM	0xbdd75a97...b32a8	0x00000000...705fa
0x06af93be...31228	13421973	2021-10-15 11:59:06 AM	0x1938a448...45ad0	0x76d338e8...3ac76

b) Immutability

As a part of a standard mining exercise, a block header is hashed repeatedly by miners by altering the nonce value to create TX hash (transaction hash) for transaction block identification as shown in the first column of tables 8-9. Through this exercise, they create a proof of work, which helps miners get rewarded for their contributions to keep the blockchain system running and ensuring a consistent state. Upon successful transaction validation, it is spread across the network with block number (Block no), Timestamp, and the Transaction hash value to ensure that it is nearly impossible to tamper. Additionally, each broadcasted block would be validated by other nodes and transactions would be checked. So any falsification could be detected easily. The figure below shows Blockchain immutability attributes.

Figure 212

Blockchain immutability attributes

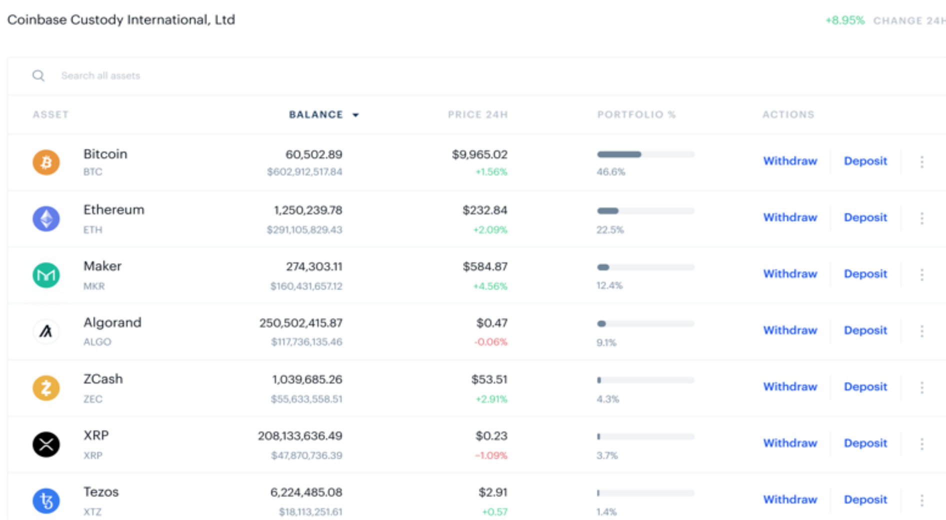


c) Decentralization

It can be confirmed that the housing transactions are recorded in a distributed ledger thus improving Transparency. Public verifiability allows anyone to verify the correct system working. Everything is archived and authorized in a decentralized way ensuring the integrity and reliable record of transactions as shown in the figure below. These records can be used by various parties (government, investors, KBS, KRA, etc.).

Figure 223

Blockchain Decentralization



Coinbase Custody International, Ltd

+8.95% CHANGE 24H

Search all assets

ASSET	BALANCE	PRICE 24H	PORTFOLIO %	ACTIONS
Bitcoin BTC	60,502.89 $602,912,517.84	$9,965.02 +1.56%	46.6%	Withdraw Deposit
Ethereum ETH	1,250,239.78 $291,105,829.43	$232.84 +2.09%	22.5%	Withdraw Deposit
Maker MKR	274,303.11 $160,431,657.12	$584.87 +4.56%	12.4%	Withdraw Deposit
Algorand ALGO	250,502,415.87 $117,736,135.46	$0.47 -0.06%	9.1%	Withdraw Deposit
ZCash ZEC	1,039,685.26 $55,633,558.51	$53.51 +2.91%	4.3%	Withdraw Deposit
XRP XRP	208,133,636.49 $47,870,736.39	$0.23 -1.09%	3.7%	Withdraw Deposit
Tezos XTZ	6,224,485.08 $18,113,251.61	$2.91 +0.57	1.4%	Withdraw Deposit

4.6 Summary

For parties to be involved in monitoring the organization's 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 is implemented in the blockchain environment to provide an open and fair tendering scheme.

CHAPTER FIVE

SUMMARY, SCONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter discusses the results of the study as per the research objectives. A summary of existing tendering models, a prototype of blockchain-based smart contract implementation to assist tendering organization, also present further areas of study and recommendations.

5.2 summary

This study was guided by the inefficiencies and weaknesses in the current management strategies in the tendering systems. Blockchain technology is explored in this research as a remedy. Due to its architecture, each tender transaction records are bundled into a block containing a unique header, and each such block is identified by its block hash (transaction hash) and other information in the blockchain parameters as discussed in chapter 2. As a part of a standard mining exercise, a block header is hashed repeatedly by miners altering the nonce value. Through this exercise, they attempt to create a proof of work, which helps miners get rewarded for their contributions to keep the blockchain system running and ensuring a consistency state. It can be confirmed that the tender transactions are recorded in a distributed ledger thus improving Transparency. Public verifiability allows anyone to evaluate the correct system working. Everything is archived and authorized in a decentralized way ensuring the integrity and reliable record of transactions. These records can be used by various parties. Enabling an efficient tendering process and providing transparency and fairness, this model satisfies the user requirements and the research objectives.

This study set out to achieve four objectives and have all been answered by the concepts summarized in the thesis, as well as the architecture of the application and the reasoning around it. The conclusion concerning each of the objectives is presented in this section and they are shortly summarized below;

5.2.1 What are the Weaknesses of E-tendering Systems?

Concerning this objective, the study sought to explore existing and proposed models used in managing to tender and investigate their weaknesses. This study analyzed three framework models including; Web-based Tendering System, E-Government Procurement systems (e-GP), Blockchain in Public Sector (Deloitte), and the Fit assessment framework for blockchain use. To achieve this, the study set out an assessment criterion as shown in Table 4 which included; objectives, benefits, and challenges of each model. Based on the assessment, this research found that none of the existing models fully satisfied the set criteria and there was a need for a new model. The E-tendering platform in Kenya is web-based and does not allow transaction transparency, immutability, or decentralization. Web-based Tendering System only focuses on ensuring anywhere anytime access of tendering adverts but Issues about openness, transparency, and non-repudiation are not addressed. On the other hand, e-Government Procurement systems (e-GP) focus on the entire procurement process without a clear blockchain-based tendering aspect. Furthermore, research carried out by Deloitte on the application of Blockchain in the Public Sector only proposes that blockchain-based solutions are suitable for tendering and the entire procurement process but it does not suggest any model for the same.

5.2.2 How will the Blockchain-Based Smart Contract Model for Tendering to be Designed?

Concerning objective two, the study sought to design a blockchain-based smart contract model for the tendering process. A design based on the model requirements and guidelines specified in the focused groups was implemented through technological methods. To write a secure and scalable smart contract back-end, the designed model as a system of smart contracts was based on the design principle of having different types of contracts to perform different classes of tasks. To classify the contracts, a model called "The Five Types Model" proposed by Monax was used. This model divides contracts into Database contracts, Controller contracts, Contract managing contracts, Application logic contracts, and Utility contracts (Monax, 2018). Based on this, the model and the PoC functional requirement, the model design resulted in the following contracts;

i. EToken contract for creating model test cryptocurrency

ii. TendertInfoDb contract for storing tender details
iii. Contract managing Contract
iv. Contract Provider contracts to coordinate testnet interactions
v. Interface contract for Dapp interaction
vi. Migrations contract for deployment

The design outlined is limited to four standard users: Admin, Biding organization, Bidder, and Third parties. To describe the various functional requirements that users have on the model, user stories from a focused group were written and are shown in Table in section 4.3.1. The user stories were simplified to the bare minimum requirements, while still keeping the PoC at a viable level of usability and security.

5.2.3 How will the Prototype of a Blockchain-Based Smart Contract Model for Tendering be Implemented?

Organizations and business enterprises depend on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. Concerning this study, the third objective pursues to implement a blockchain-based smart contract prototype for the tendering process to ensure transparency and fairness, the immutability of transaction records, and troubleshoot existing challenges in managing tenders. The developed User Registration and Authentication module were to ensure that model Participants can sign up and log inconveniently. The solidity code was implemented to allow tender creation as a smart contract for registration.

To ensure the convenience and efficient working of this model, 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 the bid evaluation code. A prospective bidder can download the tender from the blockchain. The respective bidder reviews the tender and considers the tendering specification and makes 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 developed model was deployed to an Ethereum Test Network (“testnet”), which simulates Ethereum for model testing and evaluation. The deployment steps and procedures are described in section 4. The whole code of the developed model is offered in Appendix I.

5.2.4 Can the Blockchain Model for Tendering Process Function?

Concerning objective four, the study pursued to validate and verify the implemented blockchain-based smart contract model prototype. The prototype presented in objective three was evaluated in two steps which were to, Verification to ascertain how the model overcomes the weaknesses of the existing models and validation to ascertain how the model fulfills the evaluation criteria based on user stories. Two tendering organizations were involved in the model Verification where they were allowed to interact with the model for tendering process as shown in section 4.4.1. The bidders were able to register on the organization's tender platform. They interacted with the model such that bidders submitted their proposals via the model. The organization was able to receive all bids after the deadline and submitted the evaluation results back to the model. The model was verified based on the set evaluation criteria for the existing model's evaluation which included;

i. transaction transparency
ii. immutability
iii. decentralization (distributed ledger)
iv. Non-repudiation

The model was validated using descriptive evaluation based on the model functional requirements derived from user stories as shown in table 6 of section 4.3.1. The motivation for how each of the user stories is satisfied is exposed. in Table 12. For details on the code, the reader is directed to Appendix I where the full source code can be found.

5.3 Recommendations

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 Bitcoin-like cryptocurrency, the process should include sensitizing citizens and financial organizations. This will encourage the adoption of the blockchain-based smart contracts model for tendering process among organizations.

5.4 Recommendation for Further Research

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 is implemented in the blockchain environment to provide an open and fair tendering scheme.

REFERENCES

Åkers, J. (2018). Driving fashion with data: A qualitative study of how buying firms in the buyer-driven fashion supply chain can benefit from a digitized supply chain reconfiguration.

Akbar, N. A., Muneer, A., ElHakim, N., & Fati, S. M. (2021). Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses. *Future Internet*, *13*(11), 285.

Akram, U., Fülöp, M. T., Tiron-Tudor, A., Topor, D. I., & Căpușneanu, S. (2021). Impact of digitalization on customers' well-being in the pandemic period: challenges and opportunities for the retail industry. *International Journal of Environmental Research and Public Health*, *18*(14), 7533.

Al-Bishari, K., & Khalil, R. (2021). Exploring the Efficiency of E-Tendering Services in Oman: Administrative Perspectives from Government and Business Users. In *Sustainable Production and Consumption Systems* (pp. 157-189). Springer, Singapore.

Al-Bishari, K., & Khalil, R. (2021). Exploring the Efficiency of E-Tendering Services in Oman: Administrative Perspectives from Government and Business Users. In *Sustainable Production and Consumption Systems* (pp. 157-189). Springer, Singapore.

Ahmad, T., Aljafari, R., & Venkatesh, V. (2019). The government of Jamaica's electronic procurement system: experiences and lessons learned. *Internet Research*.

Bai, C., & Sarkis, J. (2020). A supply chain transparency and sustainability technology appraisal model for blockchain technology. *International Journal of Production Research*, *58*(7), 2142-2162.

Braun-Dubler, N., Gier, H. P., Bulatnikova, T., Langhart, M., Merki, M., Roth, F., ... & Perdrisat, S. (2020). *Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment* (Vol. 73). vdf Hochschulverlag AG.

Bharosa, N., Lips, S., & Draheim, D. (2020, August). Making e-Government Work: Learning from the Netherlands and Estonia. In *International Conference on Electronic Participation* (pp. 41-53). Springer, Cham.

Baughman, R. H., Zakhidov, A. A., & De Heer, W. A. (2020). Carbon nanotubes--the route toward applications. *science*, *297*(5582), 787-792.

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, *58*(1), 102397.

Bergstra, J. A., & Burgess, M. (2018). Blockchain Technology and its Applications a Promise Theory view-V0. 11.

Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering*, *90*, 106897.

Ciotta, V., Mariniello, G., Asprone, D., Botta, A., & Manfredi, G. (2021). Integration of blockchains and smart contracts into construction information flows: Proof-of-concept. *Automation in Construction*, *132*, 103925.

Chakava, M. (2020). *Determinants of Use of New Media in Scholarly Communication by Academic Staff in Public Universities in Kenya* (Doctoral dissertation, JKUAT-COHRED).

Coelho, I. M., Coelho, V. N., Araujo, R. P., Yong Qiang, W., & Rhodes, B. D. (2020). Challenges of PBFT-inspired consensus for blockchain and enhancements over neo dBFT. *Future Internet*, *12*(8), 129.

Chan, A. P., & Owusu, E. K. (2022). Evolution of Electronic Procurement: Contemporary Review of Adoption and Implementation Strategies. *Buildings*, *12*(2), 198.

Chowdhury, N., Ramachandran, M., Third, A., Mikroyannidis, A., Bachler, M., & Domingue, J. (2020). Towards a blockchain-based decentralised educational landscape.

Ducrée, J. (2022). Satoshi Nakamoto and the Origins of Bitcoin--Narratio in Nomine, Datis et Numeris. *arXiv preprint arXiv:2206.10257*.

Dotan, M., Pignolet, Y. A., Schmid, S., Tochner, S., & Zohar, A. (2021). Survey on blockchain networking: Context, state-of-the-art, challenges. *ACM Computing Surveys (CSUR)*, *54*(5), 1-34.

Dhurandher, S. K., Singh, J., Nicopolitidis, P., Kumar, R., & Gupta, G. (2022). A blockchain-based secure routing protocol for opportunistic networks. *Journal of Ambient Intelligence and Humanized Computing*, *13*(4), 2191-2203.

Fagiolo, G., Guerini, M., Lamperti, F., Moneta, A., & Roventini, A. (2019). Validation of agent- based models in economics and finance. In *Computer Simulation Validation* (pp. 763-787). Springer, Cham.

Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications*, *177*, 102936.

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.

Guo, X., Lu, G., Villena, V. H., Vogel, D., & Heim, G. R. (2022). Supply chain transformation and technology management challenges in developing regions: Inductive theory building from rural Chinese nanostores. *Journal of Operations Management*, *68*(5), 454-486.

Gountia, D., & Satapathy, U. (2020). Security and Privacy-Enhancing Technologies for Blockchain and Cryptocurrency. In *Handbook of IoT and Blockchain* (pp. 133-150). CRC Press.

Hassija, V., Zeadally, S., Jain, I., Tahiliani, A., Chamola, V., & Gupta, S. (2021). Framework for determining the suitability of blockchain: Criteria and issues to consider. *Transactions on Emerging Telecommunications Technologies*, *32*(10), e4334.

Hamledari, H., & Fischer, M. (2021). Role of blockchain-enabled smart contracts in automating construction progress payments. *Journal of legal affairs and dispute resolution in engineering and construction*, *13*(1), 04520038.

Jayabalan, J., & Jeyanthi, N. (2021, January). A study on distributed consensus protocols and algorithms: the backbone of blockchain networks. In *2021 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-10). IEEE.

John, K., O'Hara, M., & Saleh, F. (2021). Bitcoin and beyond. *Annual Review of Financial Economics*, *14*.

Kuperberg, M., Kindler, D., & Jeschke, S. (2019). Are Smart Contracts and Blockchains Suitable for Decentralized Railway Control?. *arXiv preprint arXiv:1901.06236*.

Kabbinale, A. R., Dimogerontakis, E., Selimi, M., Ali, A., Navarro, L., &Sathiaseelan, A. (2018). Blockchain for economically sustainable wireless mesh networks. *arXiv preprint arXiv:1811.04078*.

KAFOL, C., BREGAR, A., & TRILAR, J. (2018). BLOCKCHAIN FOR ENERGY UTILITIES. *DAAAM International Scientific Book*.

Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. *Journal of Systems Architecture*, *105*, 101701.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

Kitheka, S. S. (2018). *Influence of Sourcing Ethics on Procurement Performance of State Corporations in Kenya* (Doctoral dissertation, JKUAT-COHRED).

Kurt Peker, Y., Rodriguez, X., Ericsson, J., Lee, S. J., & Perez, A. J. (2020). A cost analysis of internet of things sensor data storage on blockchain via smart contracts. *Electronics*, *9*(2), 244.

Larrucea, X., & Pautasso, C. (2020). Blockchain and Smart Contract Engineering. *IEEE Software*, *37*(5), 23-29.

Lakhanpal, V., & Samuel, R. (2018, September). Implementing Blockchain Technology in Oil and Gas Industry: A Review. In *SPE Annual Technical Conference and Exhibition*. Society of Petroleum Engineers.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, *107*, 841-853.

Kuriyama, C. A. (2018). *APEC's Bogor goals progress report*.

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.

Li, J., Greenwood, D., & Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. *Automation in Construction*, *102*, 288-307.

Lippmeier, B., Robinson, A., & Muys, A. (2019). Smart Contracts as Authorized Production Rules.

Lohachab, A., Garg, S., Kang, B., Amin, M. B., Lee, J., Chen, S., & Xu, X. (2021). Towards interconnected blockchains: a comprehensive review of the role of interoperability among disparate blockchains. *ACM Computing Surveys (CSUR)*, *54*(7), 1-39.

Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain governance—A new way of organizing collaborations?. *Organization Science*, *32*(2), 500-521.

Iyidogan, E. (2018). Incentive Mechanism and Economic Model of Blockchain Based Cryptocurrencies.

Malodia, S., Dhir, A., Mishra, M., & Bhatti, Z. A. (2021). Future of e-Government: An integrated conceptual framework. *Technological Forecasting and Social Change*, *173*, 121102.

Marthews, A., & Tucker, C. (2022). What Blockchain Can and Can't Do: Applications to Marketing and Privacy. *International Journal of Research in Marketing*.

Maulana, A., Indriati, F., & Hidayah, K. (2022). Analysis of Bureaucratic Reform Through Delayering of Government Institutions in Indonesia. *Jurnal Borneo Administrator*, *18*(2), 155-170.

Meirobie, I., Irawan, A. P., Sukmana, H. T., Lazirkha, D. P., & Santoso, N. P. L. (2022). Framework Authentication e-document using Blockchain Technology on the Government system. *International Journal of Artificial Intelligence Research*, *6*(2).

Mc Loughlin, K., Lewis, K., Lascelles, D., & Nudurupati, S. (2021). Sustainability in supply chains: reappraising business process management. *Production Planning & Control*, 1-34.

Miller, K., Miller, M., Moran, M., & Dai, B. (2018). *Data Management Life Cycle, Final report*

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.

Michaud, K. (2018). *Why Blockchain: The Complete Guide to Understanding Bitcoin and Blockchain*. Kyle Michaud.

Maheboob, K. A. S., &Mahavidyalay, V. A. P. (2019). BlockChain-An Open Distributed Ledger. *International Journal of Engineering Science*, *19672*.

Morrison, G. R., Ross, S. J., Morrison, J. R., & Kalman, H. K. (2019). *Designing effective instruction*. Wiley.

Moloi, P. M. (2018). *An exploratory study on the legitimacy of energy megaproject in South Africa* (Doctoral dissertation).

Mutangili, S. K. (2019). Influence of E-Procurement Practices on Supply Chain Performance: A Case Study of Kenya Airways. *Journal of Procurement & Supply Chain*, *3*(2), 1-16.

Nofer, M., Gomber, P., Hinz, O., &Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183-187.

Nyaberi, D. N. (2020). *Supplier Development Management Practices and Organizational Performance of Manufacturing Firms in Kenya* (Doctoral dissertation, JKUAT-COHRED).

Oluyisola, O. E., Bhalla, S., Sgarbossa, F., & Strandhagen, J. O. (2022). Designing and developing smart production planning and control systems in the industry 4.0 era: a methodology and case study. *Journal of Intelligent Manufacturing*, *33*(1), 311-332.

Pankow, K., Mosewich, A. D., & Holt, N. L. (2018). The Development of Leadership in Model Youth Football Coaches. *The Sport Psychologist*, *32*(4), 253-262.

Pradhan, N. R., Singh, A. P., Verma, S., Wozniak, M., Shafi, J., & Ijaz, M. F. (2022). A blockchain based lightweight peer-to-peer energy trading framework for secured high throughput micro-transactions. *Scientific Reports*, *12*(1), 1-15.

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking beyond banks and money* (pp. 239-278). Springer, Cham.

Qiao, L., Dang, S., Shihada, B., Alouini, M. S., Nowak, R., & Lv, Z. (2021). Can blockchain link the future?. *Digital Communications and Networks*.

Recio-Saucedo, A., Crane, K., Meadmore, K., Fackrell, K., Church, H., Fraser, S., & Blatch-Jones, A. (2022). What works for peer review and decision-making in research funding: a realist synthesis. *Research integrity and peer review*, *7*(1), 1-28.

Rotondo, A., & Quilligan, F. (2020). Evolution paths for knowledge discovery and data mining process models. *SN Computer Science*, *1*(2), 1-19.

Shi, Z., Ivankovic, V., Farshidi, S., Surbiryala, J., Zhou, H., & Zhao, Z. (2022). AWESOME: an auction and witness enhanced SLA model for decentralized cloud marketplaces. *Journal of Cloud Computing*, *11*(1), 1-25.

Silva, P., Vavricka, D., Barreto, J., & Matos, M. (2020, June). Impact of geo-distribution and mining pools on blockchains: A study of ethereum. In *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 245-252). IEEE.

Singh, K. K. (2022). Application of Blockchain Smart Contracts in E-Com

Streitz, N., & Konomi, S. I. (Eds.). (2018). *Distributed, Ambient and Pervasive Interactions: Understanding Humans: 6th International Conference, DAPI 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, July 15–20, 2018, Proceedings* (Vol. 10921). Springer.

Santos, J. P. R. (2022). *Portuguese Public Administration's eServices: The Case of Technology in the Portuguese Public Administration's Services portrayed against Estonia's reality* (Doctoral dissertation).

Santos, F. (2018). *The DAO: a million-dollar lesson in blockchain governance* (Doctoral dissertation, MA Dissertation, Talinn University of Technology, Talinn).

Sarker, T. K. (2018). *Implementing e-GP in Bangladesh: a perspective of works procurement in LGED* (Doctoral dissertation, BRAC University).

Sindiga, L. K., Paul, S. N., & Mbura, L. K. (2019). Influence of procurement management practices on performance of construction firms in Nairobi County, Kenya. *International Academic Journal of Procurement and Supply Chain Management*, *3*(1), 143-163.

Sompolinsky, Y., Wyborski, S., & Zohar, A. (2021, September). PHANTOM GHOSTDAG: a scalable generalization of Nakamoto consensus: September 2, 2021. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies* (pp. 57-70).

Stinner, J., & Tyrell, M. (2021). The New World of Blockchain Economics: Consensus Mechanism as a Core Element. In *Digitalization, Digital Transformation and Sustainability in the Global Economy* (pp. 9-19). Springer, Cham.

Takanen, A., Demott, J. D., Miller, C., & Kettunen, A. (2018). *Fuzzing for software security testing and quality assurance*. Artech House.

Tern, S. (2021). Survey of Smart Contract Technology and Application Based on Blockchain. *Open Journal of Applied Sciences*, *11*(10), 1135-1148.

Thakur, V., Doja, M. N., Dwivedi, Y. K., Ahmad, T., & Khadanga, G. (2020). Land records on blockchain for implementation of land titling in India. *International Journal of Information Management*, *52,* 101940.

Uriarte, R. B., Zhou, H., Kritikos, K., Shi, Z., Zhao, Z., & De Nicola, R. (2021). Distributed service-level agreement management with smart contracts and blockchain. *Concurrency and Computation: Practice and Experience*, *33*(14), e5800.

Wang, T., Wang, P., Cai, S., Zheng, X., Ma, Y., Jia, W., & Wang, G. (2021). Mobile edge-enabled trust evaluation for the Internet of Things. *Information Fusion*, *75*, 90-100.

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.

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).

Wehrle, K., Kira, M., & Klehe, U. C. (2019). Putting career construction into context: Career adaptability among refugees. *Journal of Vocational Behavior*, *111*, 107-124.

Yiu, N. C. (2021). An overview of forks and coordination in blockchain development. *arXiv preprint arXiv:2102.10006*.

Xiaohan, Z., & Yongqian, T. (2021, October). The Game of Capital: Prosperity or Exploitation?. In *2021 International Conference on Public Relations and Social Sciences (ICPRSS 2021)* (pp. 1228-1234). Atlantis Press.

Zhang, M., Cheng, Y., Deng, X., Wang, B., Xie, J., Yang, Y., & Zhang, J. (2021, June). Accelerating transactions relay in blockchain networks via reputation. In *2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS)* (pp. 1-10). IEEE.

Zhou, C. (2019). Instrumental Barriers to Supplying Climate Sound Technology. In *The Legal Barriers to Technology Transfer under the UN Framework Convention on Climate Change* (pp. 67-109). Springer, Singapore Office.

Zhu, Y., Zhu, M., Yang, B., Zhu, W., Deng, C., Chen, C., ... & Liu, L. (2021). Lwrpro: An energy-efficient configurable crypto-processor for module-lwr. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *68*(3), 1146-1159.

Appendix I: System Source Code

```
{
  "name": "openbid-contract",
  "version": "1.0.0",
  "description": "This project showcases the journey of transparent tender allocation on
blockchain.",
  "main": "truffle.js",
  "directories": {
    "test": "test"
  },
  "scripts": {
    "test": "echo \"test specified\" && exit 1"
  },
  "repository": {
    "type": "git",
    "url": "git+ssh://git@gitlab.com/mukira/openbid-contract.git"
  },
  "author": "Denis Kiyeng",
  "license": "ISC",
  "bugs": {
    "url": "https://gitlab.com/mukira/openbid-contract.git/issues"
  },
  "homepage": "https://gitlab.com/mukira/openbid-contract.git#README",
  "dependencies": {
    "chai": "^4.1.2",
    "eth-gas-reporter": "^0.1.7",
    "ethereumjs-abi": "^0.6.5",
    "growl": "^1.10.5",
    "truffle-hdwallet-provider": "0.0.5"
      "integrity": "sha1-2sh4dxPJlmhJ/IGAd36+nB3fO4Y="
```

```
  },
  "asn1.js": {
    "version": "4.10.1",
    "resolved": "https://registry.npmjs.org/asn1.js/-/asn1.js-4.10.1.tgz",
    "integrity": "sha512-
p32cOF5q0Zqs9uBiONKYLm6BClCoBCM5O9JfeUSlnQLBTxYdTK+pW+nXflm8Uk
Kd2UYlEbYz5qEi0JuZR9ckSw==",
    "requires": {
      "bn.js": "^4.0.0",
      "inherits": "^2.0.1",
      "minimalistic-assert": "^1.0.0"
    }
  },
  "assert": {
    "version": "1.4.1",
    "resolved": "https://registry.npmjs.org/assert/-/assert-1.4.1.tgz",
    "integrity": "sha1-mZEtWRg2tab1s0XA8H7vwI/GXZE=",
    "requires": {
      "util": "0.10.3"
    },
    "dependencies": {
      "inherits": {
        "version": "2.0.1",
        "resolved": "https://registry.npmjs.org/inherits/-/inherits-2.0.1.tgz",
        "integrity": "sha1-sX0I0ya0Qj5Wjv9xn5GwscvfafE="
      },
      "util": {
        "version": "0.10.3",
        "resolved": "https://registry.npmjs.org/util/-/util-0.10.3.tgz",
        "integrity": "sha1-evsa/lCAUkZInj23/g7TeTNqwPk=",
        "requires": {
```

```
        "inherits": "2.0.1"
      }
    }
  }
},
"assert-plus": {
  "version": "1.0.0",
  "resolved": "https://registry.npmjs.org/assert-plus/-/assert-plus-1.0.0.tgz",
  "integrity": "sha1-8S4PPF13sLHN2RRpQuTpbB5N1SU="
},
"assertion-error": {
  "version": "1.1.0",
  "resolved": "https://registry.npmjs.org/assertion-error/-/assertion-error-1.1.0.tgz",
  "integrity": "sha512-
jgsaNduz+ndvGyFt3uSuWqvy4lCnIJiovtouQN5JZHOKCS2QuhEdbcQHFhVksz2N2U9
hXJo8odG7ETyWlEeuDw=="
},
"assign-symbols": {
  "version": "1.0.0",
  "resolved": "https://registry.npmjs.org/assign-symbols/-/assign-symbols-1.0.0.tgz",
  "integrity": "sha1-WWZ/QfrdTyDMvCu5a41Pf3jsA2c="
},
"async": {
  "version": "2.6.1",
  "resolved": "https://registry.npmjs.org/async/-/async-2.6.1.tgz",
  "integrity": "sha512-
fNEiL2+AZt6AlAw/29Cr0UDe4sRAHCpEHh54WMz+Bb7QfNcFw4h3loofyJpLeQs4Y
x7yuqu/2dLgM5hKOs6HlQ==",
  "requires": {
    "lodash": "^4.17.10"
  }
```

},
"async-each": {
"version": "1.0.1",
"resolved": "https://registry.npmjs.org/async-each/-/async-each-1.0.1.tgz",
"integrity": "sha1-GdOGodntxufByF04iu28xW0zYC0="
},
"async-eventemitter": {
"version": "0.2.4",
"resolved": "https://registry.npmjs.org/async-eventemitter/-/async-eventemitter-0.2.4.tgz",
"integrity": "sha512-pd20BwL7Yt1zwDFy+8MX8F1+WCT8aQeKj0kQnTrH9WaeRETlRamVhD0JtRPmrV4GfOJ2F9CvdQkZeZhnh2TuHw==",
"requires": {
"async": "^2.4.0"
}
},
"async-limiter": {
"version": "1.0.1",
"resolved": "https://registry.npmjs.org/async-limiter/-/async-limiter-1.0.1.tgz",
"integrity": "sha512-csOlWGAcRFJaI6m+F2WKdnMKr4HhdhFVBk0H/QbJFMCr+uO2kwohwXQPxw/9OCxp05r5ghVBFSyioixx3gfkNQ=="
},
"asynckit": {
"version": "0.4.0",
"resolved": "https://registry.npmjs.org/asynckit/-/asynckit-0.4.0.tgz",
"integrity": "sha1-x57Zf380y48robyXkLzDZkdLS3k="
},
"atob": {
"version": "2.1.1",

"resolved": "https://registry.npmjs.org/atob/-/atob-2.1.1.tgz",
"integrity": "sha1-ri1acpR38onWDdf5amMUoi3Wwio="
},
"aws-sign2": {
"version": "0.7.0",
"resolved": "https://registry.npmjs.org/aws-sign2/-/aws-sign2-0.7.0.tgz",
"integrity": "sha1-tG6JCTSpWR8tL2+G1+ap8bP+dqg="
},
"aws4": {
"version": "1.7.0",
"resolved": "https://registry.npmjs.org/aws4/-/aws4-1.7.0.tgz",
"integrity": "sha512-
32NDda82rhwD9/JBCCkB+MRYDp0oSvlo2IL6rQWA10PQi7tDUM3eqMSltXmY+Oyl
/7N3P3qNtAlv7X0d9bI28w=="
},
"babel-code-frame": {
"version": "6.26.0",
"resolved": "https://registry.npmjs.org/babel-code-frame/-/babel-code-frame-
6.26.0.tgz",
"integrity": "sha1-Y/1D99weO7fONZR9uP42mj9Yx0s=",
"requires": {
"chalk": "^1.1.3",
"esutils": "^2.0.2",
"js-tokens": "^3.0.2"
}
},
"babel-core": {
"version": "6.26.3",
"resolved": "https://registry.npmjs.org/babel-core/-/babel-core-6.26.3.tgz",

"integrity": "sha512-
6jyFLuDmeidKmUEb3NM+/yawG0M2bDZ9Z1qbZP59cyHLz8kYGKYwpJP0UwUKK
UiTRNvxfLesJnTedqczP7cTDA==",
"requires": {
"babel-code-frame": "^6.26.0",
"babel-generator": "^6.26.0",
"babel-helpers": "^6.24.1",
"babel-messages": "^6.23.0",
"babel-register": "^6.26.0",
"babel-runtime": "^6.26.0",
"babel-template": "^6.26.0",
"babel-traverse": "^6.26.0",
"babel-types": "^6.26.0",
"babylon": "^6.18.0",
"convert-source-map": "^1.5.1",
"debug": "^2.6.9",
"json5": "^0.5.1",
"lodash": "^4.17.4",
"minimatch": "^3.0.4",
"path-is-absolute": "^1.0.1",
"private": "^0.1.8",
"slash": "^1.0.0",
"source-map": "^0.5.7"
}
},
"babel-generator": {
"version": "6.26.1",
"resolved": "https://registry.npmjs.org/babel-generator/-/babel-generator-6.26.1.tgz",
"integrity": "sha512-
HyfwY6ApZj7BYTcJURpM5tznulaBvyio7/0d4zFOeMPUmfxkCjHocCuoLa2SAGzBI8
AREcH3eP3758F672DppA==",

```
    "requires": {
      "babel-messages": "^6.23.0",
      "babel-runtime": "^6.26.0",
      "babel-types": "^6.26.0",
      "detect-indent": "^4.0.0",
      "jsesc": "^1.3.0",
      "lodash": "^4.17.4",
      "source-map": "^0.5.7",
      "trim-right": "^1.0.1"
    },
    "dependencies": {
      "jsesc": {
        "version": "1.3.0",
        "resolved": "https://registry.npmjs.org/jsesc/-/jsesc-1.3.0.tgz",
        "integrity": "sha1-RsP+yMGJKxKwgz25vHYiF226s0s="
      }
    }
  },
  "babel-helper-builder-binary-assignment-operator-visitor": {
    "version": "6.24.1",
    "resolved": "https://registry.npmjs.org/babel-helper-builder-binary-assignment-
operator-visitor/-/babel-helper-builder-binary-assignment-operator-visitor-6.24.1.tgz",
    "integrity": "sha1-zORReto1b0IgvK6KAsKzRvmlZmQ=",
    "requires": {
      "babel-helper-explode-assignable-expression": "^6.24.1",
      "babel-runtime": "^6.22.0",
      "babel-types": "^6.24.1"
    }
  },
  "babel-helper-call-delegate": {
    "version": "6.24.1",
```

"resolved": "https://registry.npmjs.org/babel-helper-call-delegate/-/babel-helper-call-delegate-6.24.1.tgz",
"integrity": "sha1-7Oaqzdx25Bw0YfiL/Fdb0Nqi340=",
"requires": {
"babel-helper-hoist-variables": "^6.24.1",
"babel-runtime": "^6.22.0",
"babel-traverse": "^6.24.1",
"babel-types": "^6.24.1"
}
},
"babel-helper-define-map": {
"version": "6.26.0",
"resolved": "https://registry.npmjs.org/babel-helper-define-map/-/babel-helper-define-map-6.26.0.tgz",
"integrity": "sha1-pfVtq0GiX5fstJjH66ypgZ+Vvl8=",
"requires": {
"babel-helper-function-name": "^6.24.1",
"babel-runtime": "^6.26.0",
"babel-types": "^6.26.0",
"lodash": "^4.17.4"
}
},
"babel-helper-explode-assignable-expression": {
"version": "6.24.1",
"resolved": "https://registry.npmjs.org/babel-helper-explode-assignable-expression/-/babel-helper-explode-assignable-expression-6.24.1.tgz",
"integrity": "sha1-8luCz33BBDPFX3BZLVdGQArCLKo=",
"requires": {
"babel-runtime": "^6.22.0",
"babel-traverse": "^6.24.1",
"babel-types": "^6.24.1"

    }
  },
  "babel-helper-function-name": {
    "version": "6.24.1",
    "resolved": "https://registry.npmjs.org/babel-helper-function-name/-/babel-helper-function-name-6.24.1.tgz",
    "integrity": "sha1-00dbjAPtmCQqJbSDUasYOZ01gKk=",
    "requires": {
      "babel-helper-get-function-arity": "^6.24.1",
      "babel-runtime": "^6.22.0",
      "babel-template": "^6.24.1",
      "babel-traverse": "^6.24.1",
      "babel-types": "^6.24.1"
    }
  },
  "babel-helper-get-function-arity": {
    "version": "6.24.1",
    "resolved": "https://registry.npmjs.org/babel-helper-get-function-arity/-/babel-helper-get-function-arity-6.24.1.tgz",
    "integrity": "sha1-j3eCqpNAfEHTqlCQj4mwMbG2hT0=",
    "requires": {
      "babel-runtime": "^6.22.0",
      "babel-types": "^6.24.1"
    }
  },
  "babel-helper-hoist-variables": {
    "version": "6.24.1",
    "resolved": "https://registry.npmjs.org/babel-helper-hoist-variables/-/babel-helper-hoist-variables-6.24.1.tgz",
    "integrity": "sha1-HssnaJydJVE+rbyZFKc/VAi+enY=",
    "requires": {

```
      "babel-runtime": "^6.22.0",
      "babel-types": "^6.24.1"
    }
  },
  "babel-helper-optimise-call-expression": {
    "version": "6.24.1",
    "resolved": "https://registry.npmjs.org/babel-helper-optimise-call-expression/-/babel-
helper-optimise-call-expression-6.24.1.tgz",
    "integrity": "sha1-96E0J7qfc/j0+pk8VKl4gtEkQlc=",
    "requires": {
      "babel-runtime": "^6.22.0",
      "babel-types": "^6.24.1"
    }
  },
  "babel-helper-regex": {
    "version": "6.26.0",
    "resolved": "https://registry.npmjs.org/babel-helper-regex/-/babel-helper-regex-
6.26.0.tgz",
    "integrity": "sha1-MlxZ+QL4LyS3T6zu0DY5VPZJXnI=",
    "requires": {
      "babel-runtime": "^6.26.0",
      "babel-types": "^6.26.0",
      "lodash": "^4.17.4"
    }
  },
  "babel-helper-remap-async-to-generator": {
    "version": "6.24.1",
    "resolved": "https://registry.npmjs.org/babel-helper-remap-async-to-generator/-
/babel-helper-remap-async-to-generator-6.24.1.tgz",
    "integrity": "sha1-XsWBgnrXI/7N04HxySg5BnbkVRs=",
    "requires": {
```

"babel-helper-function-name": "^6.24.1",
"babel-runtime": "^6.22.0",
"babel-template": "^6.24.1",
"babel-traverse": "^6.24.1",
"babel-types": "^6.24.1"
}
},
"babel-helper-replace-supers": {
"version": "6.24.1",
"resolved": "https://registry.npmjs.org/babel-helper-replace-supers/-/babel-helper-replace-supers-6.24.1.tgz",
"integrity": "sha1-v22/5Dk40XNpohPKiov3S2qQqxo=",
"requires": {
"babel-helper-optimise-call-expression": "^6.24.1",
"babel-messages": "^6.23.0",
"babel-runtime": "^6.22.0",
"babel-template": "^6.24.1",
"babel-traverse": "^6.24.1",
"babel-types": "^6.24.1"
}
},
"babel-helpers": {
"version": "6.24.1",
"resolved": "https://registry.npmjs.org/babel-helpers/-/babel-helpers-6.24.1.tgz",
"integrity": "sha1-NHHenK7DiOXIUOWX5Yom3fN2ArI=",
"requires": {
"babel-runtime": "^6.22.0",
"babel-template": "^6.24.1"
}
},
"babel-loader": {

"version": "6.4.1",
"resolved": "https://registry.npmjs.org/babel-loader/-/babel-loader-6.4.1.tgz",
"integrity": "sha1-CzQRLVsHSKjc2/Uaz2+b1C1QuMo=",
"requires": {
"find-cache-dir": "^0.1.1",
"loader-utils": "^0.2.16",
"mkdirp": "^0.5.1",
"object-assign": "^4.0.1"
}
},
"babel-messages": {
"version": "6.23.0",
"resolved": "https://registry.npmjs.org/babel-messages/-/babel-messages-6.23.0.tgz",
"integrity": "sha1-8830cDhYA1sqKVHG7F7fbGLyYw4=",
"requires": {
"babel-runtime": "^6.22.0"
}
},
"babel-plugin-add-module-exports": {
"version": "0.2.1",
"resolved": "https://registry.npmjs.org/babel-plugin-add-module-exports/-/babel-plugin-add-module-exports-0.2.1.tgz",
"integrity": "sha1-mumh9KjcZ/DN7E9K7aHkOl/2XiU="
},
"babel-plugin-check-es2015-constants": {
"version": "6.22.0",
"resolved": "https://registry.npmjs.org/babel-plugin-check-es2015-constants/-/babel-plugin-check-es2015-constants-6.22.0.tgz",
"integrity": "sha1-NRV7EBQm/S/9PaP3XH0ekYNbv4o=",
"requires": {
"babel-runtime": "^6.22.0"

```
    }
  },
  "babel-plugin-syntax-async-functions": {
    "version": "6.13.0",
    "resolved": "https://registry.npmjs.org/babel-plugin-syntax-async-functions/-/babel-plugin-syntax-async-functions-6.13.0.tgz",
    "integrity": "sha1-ytnK0RkbWtY0vzCuCHI5HgZHvpU="
  },
  "babel-plugin-syntax-exponentiation-operator": {
    "version": "6.13.0",
    "resolved": "https://registry.npmjs.org/babel-plugin-syntax-exponentiation-operator/-/babel-plugin-syntax-exponentiation-operator-6.13.0.tgz",
    "integrity": "sha1-nufoM3KQ2pUoggGmpX9BcDF4MN4="
  },
  "babel-plugin-syntax-trailing-function-commas": {
    "version": "6.22.0",
    "resolved": "https://registry.npmjs.org/babel-plugin-syntax-trailing-function-commas/-/babel-plugin-syntax-trailing-function-commas-6.22.0.tgz",
    "integrity": "sha1-ugNgk3+NBuQBgKQ/4NVhb/9TLPM="
  },
  "babel-plugin-transform-async-to-generator": {
    "version": "6.24.1",
    "resolved": "https://registry.npmjs.org/babel-plugin-transform-async-to-generator/-/babel-plugin-transform-async-to-generator-6.24.1.tgz",
    "integrity": "sha1-ZTbjeK/2yx1VF6wOQOs+n8jQh2E=",
    "requires": {
      "babel-helper-remap-async-to-generator": "^6.24.1",
      "babel-plugin-syntax-async-functions": "^6.8.0",
      "babel-runtime": "^6.22.0"
    }
  },
```

```
    "babel-plugin-transform-es2015-arrow-functions": {
      "version": "6.22.0",
      "resolved": "https://registry.npmjs.org/babel-plugin-transform-es2015-arrow-
functions/-/babel-plugin-transform-es2015-arrow-functions-6.22.0.tgz",
      "integrity": "sha1-RSaSy3EdX3ncf4XkQM5BufJE0iE=",
      "requires": {
        "babel-runtime": "^6.22.0"
      }
    },
    "babel-plugin-transform-es2015-block-scoped-functions": {
      "version": "6.22.0",
      "resolved": "https://registry.npmjs.org/babel-plugin-transform-es2015-block-scoped-
functions/-/babel-plugin-transform-es2015-block-scoped-functions-6.22.0.tgz",
      "integrity": "sha1-u8UbSflk1wy42OC5ToICRs46YUE=",
      "requires": {
        "babel-runtime": "^6.22.0"
      }
    },
    "babel-plugin-transform-es2015-block-scoping": {
      "version": "6.26.0",
      "resolved": "https://registry.npmjs.org/babel-plugin-transform-es2015-block-
scoping/-/babel-plugin-transform-es2015-block-scoping-6.26.0.tgz",
      "integrity": "sha1-1w9SmcEwjQXBL0Y4E7CgnnOxiV8=",
      "requires": {
        "babel-runtime": "^6.26.0",
        "babel-template": "^6.26.0",
        "babel-traverse": "^6.26.0",
        "babel-types": "^6.26.0",
        "lodash": "^4.17.4"
      }
    },
```

```
  "babel-plugin-transform-es2015-classes": {
    "version": "6.24.1",
    "resolved": "https://registry.npmjs.org/babel-plugin-transform-es2015-classes/-/babel-plugin-transform-es2015-classes-6.24.1.tgz",
    "integrity": "sha1-WkxYpQyclGHlZLSyo7+ryXolhNs=",
    "requires": {
      "babel-helper-define-map": "^6.24.1",
      "babel-helper-function-name": "^6.24.1",
      "babel-helper-optimise-call-expression": "^6.24.1",
      "babel-helper-replace-supers": "^6.24.1",
      "babel-messages": "^6.23.0",
      "babel-runtime": "^6.22.0",
      "babel-template": "^6.24.1",
      "babel-traverse": "^6.24.1",
      "babel-types": "^6.24.1"
    }
  },
  "babel-plugin-transform-es2015-computed-properties": {
    "version": "6.24.1",
    "resolved": "https://registry.npmjs.org/babel-plugin-transform-es2015-computed-properties/-/babel-plugin-transform-es2015-computed-properties-6.24.1.tgz",
    "integrity": "sha1-b+Ko0WiV1WNPTNmZttNICjCBWbM=",
    "requires": {
      "babel-runtime": "^6.22.0",
      "babel-template": "^6.24.1"
    }
  },
  "babel-plugin-transform-es2015-destructuring": {
    "version": "6.23.0",
    "resolved": "https://registry.npmjs.org/babel-plugin-transform-es2015-destructuring/-/babel-plugin-transform-es2015-destructuring-6.23.0.tgz",
```

```
    "integrity": "sha1-mXux8auWf2gtKwh2/jWNYOdlxW0=",
    "requires": {
      "babel-runtime": "^6.22.0"
    }
  },
  "babel-register": {
    "version": "6.26.0",
    "resolved": "https://registry.npmjs.org/babel-register/-/babel-register-6.26.0.tgz",
    "integrity": "sha1-btAhFz4vy0htestFxgCahW9kcHE=",
    "requires": {
      "babel-core": "^6.26.0",
      "babel-runtime": "^6.26.0",
      "core-js": "^2.5.0",
      "home-or-tmp": "^2.0.0",
      "lodash": "^4.17.4",
      "mkdirp": "^0.5.1",
      "source-map-support": "^0.4.15"
    }
  },
  "babel-runtime": {
    "version": "6.26.0",
    "resolved": "https://registry.npmjs.org/babel-runtime/-/babel-runtime-6.26.0.tgz",
    "integrity": "sha1-llxwWGaOgrVde/4E/yM3vItWR/4=",
    "requires": {
      "core-js": "^2.4.0",
      "regenerator-runtime": "^0.11.0"
    }
  },
  "babel-template": {
    "version": "6.26.0",
    "resolved": "https://registry.npmjs.org/babel-template/-/babel-template-6.26.0.tgz",
```

```
    "integrity": "sha1-3gPi0WOWsGn0bdn/+FIfsaDjXgI=",
    "requires": {
      "babel-runtime": "^6.26.0",
      "babel-traverse": "^6.26.0",
      "babel-types": "^6.26.0",
      "babylon": "^6.18.0",
      "lodash": "^4.17.4"
    }
  },
  "babel-traverse": {
    "version": "6.26.0",
    "resolved": "https://registry.npmjs.org/babel-traverse/-/babel-traverse-6.26.0.tgz",
    "integrity": "sha1-RqnL1+3MYsjlwGTi0tjQ9ANXZu4=",
    "requires": {
      "babel-code-frame": "^6.26.0",
      "babel-messages": "^6.23.0",
      "babel-runtime": "^6.26.0",
      "babel-types": "^6.26.0",
      "babylon": "^6.18.0",
      "debug": "^2.6.8",
      "globals": "^9.18.0",
      "invariant": "^2.2.2",
      "lodash": "^4.17.4"
    }
  },
  "babel-types": {
    "version": "6.26.0",
    "resolved": "https://registry.npmjs.org/babel-types/-/babel-types-6.26.0.tgz",
    "integrity": "sha1-o7Bz+Uq0nrb6Vc1lInozQ4BjJJc=",
    "requires": {
      "babel-runtime": "^6.26.0",
```

"esutils": "^2.0.2",
"lodash": "^4.17.4",
"to-fast-properties": "^1.0.3"
}
},
"babelify": {
"version": "7.3.0",
"resolved": "https://registry.npmjs.org/babelify/-/babelify-7.3.0.tgz",
"integrity": "sha1-qlau3nBn/XvVSWZu4W3ChQh+iOU=",
"requires": {
"babel-core": "^6.0.14",
"object-assign": "^4.0.0"
}
},
"babylon": {
"version": "6.18.0",
"resolved": "https://registry.npmjs.org/babylon/-/babylon-6.18.0.tgz",
"integrity": "sha512-q/UEjfGJ2Cm3oKV71DJz9d25TPnq5rhBVL2Q4fA5wcC3jcrdn7+SssEybFIxwAvvP+YCsCYNKughoF33GxgycQ=="
},
"backoff": {
"version": "2.5.0",
"resolved": "https://registry.npmjs.org/backoff/-/backoff-2.5.0.tgz",
"integrity": "sha1-9hbtqdPktmuMp/ynn2lXIsX44m8=",
"requires": {
"precond": "0.2"
}
},
"balanced-match": {
"version": "1.0.0",

"resolved": "https://registry.npmjs.org/balanced-match/-/balanced-match-1.0.0.tgz",
"integrity": "sha1-ibTRmasr7kneFk6gK4nORi1xt2c="
},
},
"dependencies": {
"ethereumjs-util": {
"version": "5.2.0",
"resolved": "https://registry.npmjs.org/ethereumjs-util/-/ethereumjs-util-5.2.0.tgz",
"integrity": "sha512-
CJAKdI0wgMbQFLlLRtZKGcy/L6pzVRgelIZqRqNbuVFM3K9VEnyfbcvz0ncWMRN
Ce4kaHWjwRYQcYMucmwsnWA==",
"requires": {
"bn.js": "^4.11.0",
"create-hash": "^1.1.2",
"ethjs-util": "^0.1.3",
"keccak": "^1.0.2",
"rlp": "^2.0.0",
"safe-buffer": "^5.1.1",
"secp256k1": "^3.0.1"
}
},
"keccak": {
"version": "1.4.0",
"resolved": "https://registry.npmjs.org/keccak/-/keccak-1.4.0.tgz",
"integrity": "sha512-
eZVaCpblK5formjPjeTBik7TAg+pqnDrMHIffSvi9Lh7PQgM1+hSzakUeZFCk9DVVG
0dacZJuaz2ntwlzZUIBw==",
"requires": {
"bindings": "^1.2.1",
"inherits": "^2.0.3",
"nan": "^2.2.1",

```
          "safe-buffer": "^5.1.0"
        }
      }
    }
  },
  "webpack": {
    "version": "2.7.0",
    "resolved": "https://registry.npmjs.org/webpack/-/webpack-2.7.0.tgz",
    "integrity": "sha512-
MjAA0ZqO1ba7ZQJRnoCdbM56mmFpipOPUv/vQpwwfSI42p5PVDdoiuK2AL2FwFU
VgT859Jr43bFZXRg/LNsqvg==",
    "requires": {
      "acorn": "^5.0.0",
      "acorn-dynamic-import": "^2.0.0",
      "ajv": "^4.7.0",
      "ajv-keywords": "^1.1.1",
      "async": "^2.1.2",
      "enhanced-resolve": "^3.3.0",
      "interpret": "^1.0.0",
      "json-loader": "^0.5.4",
      "json5": "^0.5.1",
      "loader-runner": "^2.3.0",
      "loader-utils": "^0.2.16",
      "memory-fs": "~0.4.1",
      "mkdirp": "~0.5.0",
      "node-libs-browser": "^2.0.0",
      "source-map": "^0.5.3",
      "supports-color": "^3.1.0",
      "tapable": "~0.2.5",
      "uglify-js": "^2.8.27",
      "watchpack": "^1.3.1",
```

```
    "webpack-sources": "^1.0.1",
    "yargs": "^6.0.0"
  },
  "dependencies": {
    "ajv": {
      "version": "4.11.8",
      "resolved": "https://registry.npmjs.org/ajv/-/ajv-4.11.8.tgz",
      "integrity": "sha1-gv+wKynmYq5TvcIK8VlHcGc5xTY=",
      "requires": {
        "co": "^4.6.0",
        "json-stable-stringify": "^1.0.1"
      }
    },
    "supports-color": {
      "version": "3.2.3",
      "resolved": "https://registry.npmjs.org/supports-color/-/supports-color-3.2.3.tgz",
      "integrity": "sha1-ZawFBLOVQXHYpklGsq48u4pfVPY=",
      "requires": {
        "has-flag": "^1.0.0"
      }
    },
    "yargs": {
      "version": "6.6.0",
      "resolved": "https://registry.npmjs.org/yargs/-/yargs-6.6.0.tgz",
      "integrity": "sha1-eC7CHvQDNF+DCoCMo9UTr1YGUgg=",
      "requires": {
        "camelcase": "^3.0.0",
        "cliui": "^3.2.0",
        "decamelize": "^1.1.1",
        "get-caller-file": "^1.0.1",
        "os-locale": "^1.4.0",
```

```
          "read-pkg-up": "^1.0.1",
          "require-directory": "^2.1.1",
          "require-main-filename": "^1.0.1",
          "set-blocking": "^2.0.0",
          "string-width": "^1.0.2",
          "which-module": "^1.0.0",
          "y18n": "^3.2.1",
          "yargs-parser": "^4.2.0"
        }
      },
      "yargs-parser": {
        "version": "4.2.1",
        "resolved": "https://registry.npmjs.org/yargs-parser/-/yargs-parser-4.2.1.tgz",
        "integrity": "sha1-KczqwNxPA8bIe0qfIX3RjJ90hxw=",
        "requires": {
          "camelcase": "^3.0.0"
        }
      }
    }
  },
  "webpack-sources": {
    "version": "1.1.0",
    "resolved": "https://registry.npmjs.org/webpack-sources/-/webpack-sources-
1.1.0.tgz",
    "integrity": "sha512-
aqYp18kPphgoO5c/+NaUvEeACtZjMESmDChuD3NBciVpah3XpMEU9VAAtIaB1Bsf
JWWTSdv8Vv1m3T0aRk2dUw==",
    "requires": {
      "source-list-map": "^2.0.0",
      "source-map": "~0.6.1"
    },
```

```
    "dependencies": {
      "source-map": {
        "version": "0.6.1",
        "resolved": "https://registry.npmjs.org/source-map/-/source-map-0.6.1.tgz",
        "integrity": "sha512-
UjgapumWlbMhkBgzT7Ykc5YXUT46F0iKu8SGXq0bcwP5dz/h0Plj6enJqjz1Zbq2l5Wa
qYnrVbwWOWMyF3F47g=="
      }
    }
  },
  "whatwg-fetch": {
    "version": "2.0.4",
    "resolved": "https://registry.npmjs.org/whatwg-fetch/-/whatwg-fetch-2.0.4.tgz",
    "integrity": "sha512-
dcQ1GWpOD/eEQ97k66aiEVpNnapVj90/+R+SXTPYGHpYBBypfKJEQjLrvMZ7YXb
Km21gXd4NcuxUTjiv1YtLng=="
  },
  "which-module": {
    "version": "1.0.0",
    "resolved": "https://registry.npmjs.org/which-module/-/which-module-1.0.0.tgz",
    "integrity": "sha1-u6Y8qGGUiZT/MHc2CJ47lgJsKk8="
  },
  "wordwrap": {
    "version": "0.0.2",
    "resolved": "https://registry.npmjs.org/wordwrap/-/wordwrap-0.0.2.tgz",
    "integrity": "sha1-t5Zpu0LstAn4PVg8rVLKF+qhZD8="
  },
  "wrap-ansi": {
    "version": "2.1.0",
    "resolved": "https://registry.npmjs.org/wrap-ansi/-/wrap-ansi-2.1.0.tgz",
    "integrity": "sha1-2Pw9KE3QV5T+hJc8rs3Rz4JP3YU=",
```

```
    "requires": {
      "string-width": "^1.0.1",
      "strip-ansi": "^3.0.1"
    }
  },
  "wrappy": {
    "version": "1.0.2",
    "resolved": "https://registry.npmjs.org/wrappy/-/wrappy-1.0.2.tgz",
    "integrity": "sha1-tSQ9jz7BqjXxNkYFvA0QNuMKtp8="
  },
  "ws": {
    "version": "5.2.2",
    "resolved": "https://registry.npmjs.org/ws/-/ws-5.2.2.tgz",
    "integrity": "sha512-
jaHFD6PFv6UgoIVda6qZllptQsMlDEJkTQcybzzXDYM1XO9Y8em691FGMPmM46W
GyLU4z9KMgQN+qrux/nhlHA==",
    "requires": {
      "async-limiter": "~1.0.0"
    }
  },
  "xhr": {
    "version": "2.5.0",
    "resolved": "https://registry.npmjs.org/xhr/-/xhr-2.5.0.tgz",
    "integrity": "sha512-
4nlO/14t3BNUZRXIXfXe+3N6w3s1KoxcJUUURctd64BLRe67E4gRwp4PjywtDY72fX
pZ1y6Ch0VZQRY/gMPzzQ==",
    "requires": {
      "global": "~4.3.0",
      "is-function": "^1.0.1",
      "parse-headers": "^2.0.0",
      "xtend": "^4.0.0"
```

```
    }
  },
  "xhr2": {
    "version": "0.1.4",
    "resolved": "https://registry.npmjs.org/xhr2/-/xhr2-0.1.4.tgz",
    "integrity": "sha1-f4dliEdxbbUCYyOBL4GMras4el8="
  },
  "xmlhttprequest": {
    "version": "1.8.0",
    "resolved": "https://registry.npmjs.org/xmlhttprequest/-/xmlhttprequest-1.8.0.tgz",
    "integrity": "sha1-Z/4HXFwk/vOfnWX197f+dRcZaPw="
  },
  "xtend": {
    "version": "4.0.1",
    "resolved": "https://registry.npmjs.org/xtend/-/xtend-4.0.1.tgz",
    "integrity": "sha1-pcbVMr5lbiPbgg77lDofBJmNY68="
  },
  "y18n": {
    "version": "3.2.1",
    "resolved": "https://registry.npmjs.org/y18n/-/y18n-3.2.1.tgz",
    "integrity": "sha1-bRX7qITAhnnA136I53WegR4H+kE="
  }
 }
}
```

Appendix II: University Research Authorization

KABARAK UNIVERSITY

Private Bag - 20157
KABARAK, KENYA
Tel: 0773 265 999

BOARD OF POSTGRADUATE STUDIES

17th ***February 2020***

The Director General
National Commission for Science, Technology & Innovation (NACOSTI)
P.O. Box 30623 – 00100
NAIROBI

Dear Sir/Madam,

RE: DENIS K. KIYENG (GMIA/N/0824/05/16)

The above named is a Masters Student at Kabarak University in the School of Science Engineering and Technology He is carrying out a research entitled ***"A Blockchain Based Smart Contract Model for Tendering"***. He has defended his proposal and has been authorized to proceed with field research.

The information obtained in the course of this research will be used for academic purposes only and will be treated with utmost confidentiality.

Please provide him with a research permit to enable him to undertake his research.

KABARAK UNIVERSITY DIRECTOR POST GRADUATE STUDIES 17 FEB 2020 PRIVATE BAG - 20157, KABARAK

Thank you.

Yours faithfully,

Dr. Wilson Shitandi
AG. DIRECTOR, INSTITUTE OF POSTGRADUATE STUDIES (IPGS)

Kabarak University Moral Code

As members of Kabarak University family, we purpose at all times and in all place to set apart in one's heart, Jesus as Lord. (1 Peter 3:15)

Kabarak University is ISO 9001:2015 Certified

Appendix III: Guidelines For Conducting The Focus Group

The statement of purpose

The Focus group discussion approach in this research aims to define the projected model's requirements and to validate the model based on the discussed feature. It aims to obtain data from a purposely-selected group of individuals with experience in blockchain and distributed applications development.

Sampling Procedures for Focus Groups

The focus group will be taking between 4-7 members per group as guided by Krueger and Casey (2002).The goal of the study is taken into account while deciding who to invite to the group interview. Members of the focus groups are also chosen based on their knowledge. Members with blockchain and distributed application development experience are the ideal candidates. In the focus group, a homogeneous audience is a goal.

Focus group pattern

The pattern for introducing the group discussion includes: 1) Welcome, 2) Overview of the topic, 3) Ground rules and 4) the First question.

Appendix IV: Official Receipt For Payment Of Research Permit

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

AC 04158

OFFICIAL RECEIPT

Station: Nairobi **Date:** 20/Mar/2020

Received from: Denis Kipkemoi Kiyeng

KES: *** One Thousand only ***

On Account of Research Permit Fees ref 04711

Vote Head R-43

USD	
Kshs	1,000
AC	
NO	

Item A-1-A

Cash/Cheque No MPESA

Appendix V: Research Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **907516**

Date of Issue: **27/March/2020**

RESEARCH LICENSE

This is to Certify that Mr.. Denis Kipkemoi Kiyeng of Kabarak University, has been licensed to conduct research in Nakuru on the topic: A BLOCKCHAIN BASED SMART CONTRACT MODEL FOR TENDERING for the period ending : 27/March/2021.

License No: **NACOSTI/P/20/4657**

907516

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

Appendix VI: Organizations With Certified Processes for Sample Frame

Kenya Bureau of Standards

Standards for Quality life

	Firm Name	Postal Address	Cert No	Scope Cert	Issue Date	Expiry Date
1.	Rift Valley Institute of science and Technology	P O Box 7182-20100, Nakuru Kenya	QMS/171	Provision of Technical, Vocational Education and training	13th January 2013	12th January 2022
2.	Nakuru Water & Sanitation Co. Ltd	P.O. Box 16314-20100, Nakuru	QMS/291	Provision of Water, Sewerage, Water Testing and Water Meter Calibration Services	23th January 2016	22nd January 2020
3.	National Irrigation Board	P.O. Box 30372-00100	QMS/136	Development, promotion and improvement of irrigation and irrigated crops	13th May 2019	12th May 2022
4.	Public Procurement Regulatory Authority (PPRA	P.O Box 785 – 20100, Nakuru	QMS/273	Regulation of the Public Procurement and assets disposals systems in Kenya	25th September 2018	24th September 2021
5.	National Construction Authority	Former Ministry of Public Works Offices Prison Road, *Nakuru*. +254 708 768 457.	QMS/300	Regulation of Construction Industry	3rd November 2020	10th October 2023
6.	Energy and Petroleum Regulatory Authority	P.O Box 785 – 20100 Nakuru	QMS/116	Regulation of the Electric Power, Petroleum and Renewable Energy Sectors in Kenya	28th June 2010	25th August 2022
7.	Jomo Kenyatta University of Agriculture and Technology	P.O. Box 1063 – 20100, Nakuru	QMS/096	Provision of higher education, research and Innovation	29th July 2009	29th July 2021
8.	Kabarak	Private Bag -	QMS/307	Provision of Higher	21st	6th

Kenya Bureau of Standards
Standards for Quality life

	University	20157, KABARAK		Education	December 2020	November 2023
9.	National Hospital Insurance Fund	P.O. Box 155-20100 Nakuru	QMS/062	Provision of Health Insurance in Kenya	15th April 2019	21st July 2021
10.	Kenya Breweries limited	P.O Box 707-20100, Nakuru	QMS/004	Production of beer, Cider, spirit, adult non-alcoholic beverages (ANADS) and ready to drink spirit based products from receipt of raw materials to the dispatch of finished goods	20th July 2006	19th July 2022
11.	Kenya National Highways Authority	P O Box 492-20100, Nakuru	QMS/ 224	Management, development, rehabilitation and Maintenance of national trunk roads(Class A, B and C)	3rd July 2013	2nd July 2022
12.	Kenya Railways corporation	P.O. Box 3121-20100, Nakuru	QMS/345	Management and supervision of rail transportation (SGR), rail infrastructure development and provision of real estate services?	12th January 2021	11th January 2024
13.	Unga Farm Care(EA) Limited	P.O BOX 3038 – 20100 Nakuru	QMS/321	Manufacture of animal feeds.	27th November 2018	26th November 2021
14.	LAIKIPIA UNIVERSITY	P.O BOX 1100-20100, Nakuru	QMS/332	Design, Development and delivery of teaching, learning,	8th August 2019	7th August 2022

				research, innovation and community service		
15.	Kenya Urban Roads Authority	P.O. Box 4177-20100, Nakuru	QMS.236	Management, development, rehabilitation and mantainace of national urban trunk roads in Kenya.	11th June 2015	10th June 2021

Appendix VII: Sample Report Of Kenya National Highway Authority

KeNHA Kenya National Highways Authority

Quality Highways, Better Connections

Provincial Public Works Building, **P.O Box** 17752- 20100, Nakuru. **Tel:** 0785 663 908

Email: rd.southrift@kenha.co.ke **Website:** www.kenha.co.ke

TO WHOM IT MAY CONCERN

RE: <u>DENIS KIYENG MODEL TEST</u>

This is to confirm that the above name person tested the research model on the application of blockchain and smart contract technology in tendering June 2020.

Attached is a transaction record showing interaction with the model.

Yours Faithfully,

Enock Rotich

ICT Assistant

Kenya National Highways Authority
SOUTH RIFT REGION
ICT DEPARTMENT
3 0 JUN 2020
P. O. Box 17752-20100,
NAKURU

TX hash	Block no	Timestamp	Date Time	From	To	Quantity
0xa4d7c7bd345a0e5da7bf06bad29a9a5aad8fa 3a6da2dd8ac4a22facced772ca	5102742	1551299082	6/29/2020 11:00	0xa6e532bb14d444a4a7146 14/260453609018c96c	0x32cd37a01a62960585 0 7d1f018c8db8676a90aaf	3000
0x8f2e22c99ab613f2720106208c82 51ba2669a3dd5dd83c5119bd7dd41559475	5137983	1551718836	6/29/2020 11:05	0x0189bf742d56e94dd047b a09185c5e139b35b2f	0x32cd37a01a6296058507 d1f018c8db8676a90aaf	2300
0x315d74a791457a8ac5c9a176a30a 98304f3d1517606dc335648a8060f03516	5234443	1552992760	6/29/2020 11:30	0x13a7b6833a25c19b9d19ba 3153bb95c173a8d34	0x32cd37a01a6296058507 d1f018c8db8676a90aaf	1700
0xdf187bd3a83f16028193ed3b4 b91b8e02e9fa2ed28f93c36c5f93336aacf8b02a1	5235275	1553003197	6/30/2020 12:10	0x13e7b6833e25c19b9d19 be3153bb95c173af8d34	0x32cd37a01a6296058507 d1f018c8db8676a90aaf	1100
0xa799b13f9150e48c8bf8c85e03c0ee d0a72c85ed0b8243865ed1d1dcefbd5217	5235278	1553003214	6/30/2020 12:13	0x13e7b6833e25e19b9d19b a3153bb95c173af3d34	0x32cd37a01a62960585 0 7d1f018c8db8676a90aaf	2000
0x4e4b945584ebb863b3a648b70d00 7130cb4f214294f72fa28d39122f94e07962	5235449	1553005518	6/30/2020 12:15	0x13e7b6833e25e19b9d19b a3153be95c173af3d34	0x32cd37a01a62960585 0 7d1f018c8db8676a90aaf	2700
0x6893fa0148737bda6977e728a871 1b8ed8814fb6e9593a343681e55a67bf99ae6	5710843	1559395986	6/30/2020 12:16	0xabd5872aa4d1c85a03a58 1127b872c99ebbab000	0x32cd37a01a62960585 0 7d1f018c8db8676a90aaf	1900
0x6893fa0148757bda6977e728a871 1b8ed8814fb6e9593a343681e55a67bf99ae6	5710843	1559395986	6/30/2020 12:17	0xebd3872aa4d1c85a03a58 1127b872a99ebbeb000	0x32cd37a01a62960585 0 7d1f018c8db8676a90aaf	1500
0xa799b13f9150e48c8bf8c85e03c0ee d0a72c85ed0b8243865ed1d1dcefbd5217	5235278	1553003214	6/30/2020 12:19	0x13e7b6833e25e19b9d19b a3153bb95c173af3d34	0x32cd37a01a62960585 0 7d1f018c8db8676a90aaf	2000
0x4e4b945584bb863b3a648b70d00 7130cb4f214294f72fa28d39122f94e07962	5235449	1553005518	6/30/2020 12:20	0x13e7b6833e25e19b9d19b a3153bb95c173af3d34	0x32cd37a01a62960585 0 7d1f018c8ab8676a90aaf	2760
0x6893fa0148757bda6977e728a871 1b8ec8814fb6e9593a343681e55e67bf99ae6	5710843	1559395986	6/30/2020 12:22	0xabd5872aa4d1c85a03a58 1127b872c99ebbeb000	0x32cd37a01a62960585 0 7d1f018c8db8676a90aaf	[illegible]
0x6893fa0148737bda6977e728a871 1b8ed8814fb6e9593a343681e55a67bf99ae6	5710843	1559395986	6/30/2020 12:23	0xabd3872aa4d1c85a03a58 1127b872c99ebbeb000	0x32cd37a01a62960585 0 7d1f018c8db8676a90aaf	[illegible]

Kenya National Highways Authority
SOUTH RIFT REGION
ICT DEPARTMENT
30 JUN 2020
P. O. Box 17752-20100,
NAKURU

Appendix VIII: Sample Report Of Unga Farm Care Limited

UNGA
FARM CARE (EA) LIMITED
Alama ya Ubora

P.O. Box 3038 – 20100
Nakuru, Kenya
Physical Location:
Commercial Street Industrial Area

Phone: +254 335 5772
Email: ul@unga.com
Website: unga-group.com

Procurement & Sales Lead, Rift Region

23rd JULY 2020

TO WHOM IT MAY CONCERN

RE: DENIS KIYENG BLOCKCHAIN FOR TENDER MODEL TEST

This is to confirm that the above name person tested the research model on the application of blockchain and smart contract technology in tendering June 2020.

Attached is a transaction record showing interaction with the MODEL

Regards

UNGA FARM CARE
NAKURU
23 JUL 2020

Mr. Egadwa Gazembe
Procurement & Sales Lead, Rift Region
Email: egazembe@unga.com
Phone: +254 335 5772

TX hash	Block no	Timestamp	Date Time	From	To	Quantity
0xe9912a22c99a1613f2720104f2f08c82 51ba0669a3465d183e5119bd7dd41559479	3147880	10551259085 1551259083	7/11/2020 10:00	0xc6a552bb14d44c4af346 14f7004531609018c96c	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	3000
0xa7df7c7bd246a0e5de7bfd86ac29c9a5cadffa 3a6da2dd8ac4e22faccd772ca	3147885	10551718883 1551718838	7/11/2020 10:00	0x0259bd742d56e944d8047b a09195c5a139b35b2f	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	2200
0xe415d74a791457efac5c9a176a30e 9839f5d151760064de335648a8069f0f3316	3147886	10552992278 1552992768	7/11/2020 10:06	0x13e7b6833e25e19b9d19ba 3153bb95c173afdd34	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	3800
0xdd677bd3a83f16628f0d7b4 b91b8c02c9fa2e0d2895b26e5b93336aca5b02a1	3147887	10553003319 1553003192	7/11/2020 10:08	0x13e7b6833e25e19b9d19 ba3153bb95c173afdd34	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	2200
0xa679b13f9150e49c8bf8c85e09c0ee d0c72c85ac0b8243865ad1d1dcefbd5217	3147888	10553003329 1553003214	7/11/2020 10:08	0x13e7b6833e25e19b9d19b a3153bb695c173afdd34	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	3100
0xc4e4b945584bb863b3a648b70e00 7130db4f214294f72fe2f8d39322f94c979b2	3147890	10553005559 1553005518	7/11/2020 10:39	0x13e7b6833e25e19b9d19b a3153bb695c173afdd34	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	1800
0x6738c0148757bdc6977d728a871 1b8ec8814f6e9593a343681c55a67bf69ac6	3147891	10559939998 1559939986	7/11/2020 10:35	0xebd3872ea4d1d85a03a58 1127b872c99ebbab000	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	3300
0x6738c0148757bdc6977d728a871 1b8ec8814f6e9593a343681c55a67bf69ac6	3147893	10559939999 1559939986	7/11/2020 10:38	0xebd3872ea4d1d85a03a58 1127b872c99ebbab000	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	4000
0xa679b13f9150e49c8bf8c85e09c0ee d0c72c85ac0b8243865ad1d1dcefbd5217	3147894	10553003340 1553003210	7/11/2020 10:38	0x13e7b6833e25e19b9d19b a3153bb695c173afdd34	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	2800
0xc4e4b945584bb863b3a648b70e00 7130db4f214294f72fe2f8d39322f94c979b2	3147895	10553005550 1553005518	7/11/2020 10:40	0x13e7b6833e25e19b9d19b a3153bb695c173afdd34	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	1700
0x6738c0148757bdc6977d728a871 1b8ec8814f6e9593a343681c55a67bf69ac6	3147897	10559939599 1559939988	7/11/2020 10:41	0xebd3872ea4d1d85a03a58 1127b872c99ebbab000	0x32ed37a01a628605850 7d1f018c8cb8676a90aaf	3100
0x6738c0148757bdc6977d728a871 1b8ec8814f6e9593a343681c55a67bf69ac6	3147898	10559939998 1559939984	7/11/2020 10:45	0xebd3872ea4d1d85a03a58 1127b872c99ebbab000	0x32ed37a01a62[illegible] 7d1f018c8cb8[illegible]	3500
0xc4e4b945584bb863b3a648b70e00 7130db4f214294f72fe2f8d39322f94c979b2	3147895	1553005518	7/11/2020 10:26	0x13e7b6833e25e19b9d19b a3153bb95c173afdd34	0x32ed37a0[illegible] 7d1f018c8cb[illegible]6a90aaf	2700
0x6738c0148757bdc6977d728a871 1b8ec8814f6e9593a343681c55a67bf69ac6	3147897	1559939986	7/11/2020 10:27	0xebd3872ea4d1d85a03a58 1127b872c99ebbab000	0x32ed37a01a62[illegible] 7d1f018c8cb[illegible]a90aaf	1200
0x6738c0148757bdc6977d728a871 1b8ec8814f6e9593a343681c55a67bf69ac6	3147898	1559939986	7/11/2020 10:28	0xebd3872ea4d1d85e03a58 1127b872c99ebbab000	0x32ed37a01a628605850 7d1f018c8cb8676[illegible]	2500

Appendix IIX: Research Publication I

International Journal of Computer Applications Technology and Research
Volume 10–Issue 10, 222-225, 2021, ISSN:-2319–8656

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 21st 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 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).