A MODEL FOR CREATING A STABLE CRYPTOCURRENCY USING FIAT CURRENCY FOR GLOBAL ELECTRONIC COMMERCE

ALEX KIBET

A Thesis Submitted to the Institute of Postgraduate Studies for Partial Fulfilment for the Requirements for the Award of Doctor of Philosophy in Information Technology.

KABARAK UNIVERSITY

NOVEMBER, 2022

DECLARATION

1. I do declare that:

(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) That the work has not in-cooperated material from other works or a paraphrase of such material without due and appropriate acknowledgment

(iii) That the work has been subjected to processes of anti-plagiarism and has met Kabarak University's 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

Signed: _____Date: _____

Name of Student: **ALEX KIBET** Admission Number: **GDI/N/0430/01/20**

RECOMMENDATION

To the Institute of Postgraduate Studies:

The thesis entitled **"A Model for Creating Stable Cryptocurrency Using Fiat Currency for Global Electronic Commerce"** and written by **Alex Kibet** is presented to the Institute of Postgraduate Studies of Kabarak University. We have reviewed the research thesis and recommend it be accepted in partial fulfillment of the requirement for the award of the degree of Doctor of Philosophy in Information Technology.

Signed: _____ Date: _____

Prof. Simon Karume

Department of Computer Science & Information Technology

Kabarak University

Signed: _____ Date: _____

Dr. Nelson Masese

Department of Computer Science & Information Technology

Kabarak University

COPYRIGHT

ACKNOWLEDGMENTS

Firstly, I wish to acclaim God for the endowment of life and arrangement without which I would not have made it this far in my scholastic interests. In reality, the capacity to peruse and understand is a blessing that in solitary only God gives. All honor, commendation, and magnificence are to God. Secondly, I would wish to thank the whole of Kabarak University for the occasion to concentrate on Kabarak and all the help that they gave me during my studies. In addition, I am deeply indebted to the Institute of Postgraduate Studies, The School of Science Engineering and Technology, and the Department of Computer Science & Information Technology of Kabarak University for the Support I received during my studies.

Furthermore, I would like to express my sincere gratitude to my supervisors Prof. Simon Karume and Dr. Nelson Masese for their steady help during the thesis writing. Their understanding, motivation, huge information sharing, insightful guidance, and contribution during my exploration have made the composition of this research conceivable. As my teachers and mentors, they have shown me beyond what I would give them credit for here. They have shown me, by their example, what a good scientist (and person) should be. Other than my supervisors, I also want to thank all those whom I have had the delight to work with during this and other related scholarly angles. I am appreciative of my cohorts Komen, Jared, Leah, and Tony for their clever remarks and consolation as well as for the hard inquiry, which incented me to augment my exploration from different viewpoints. No one has been more critical of me chasing my investigations than the individuals from my family. I also want to thank my folks; whose affection and direction are with me in whatever I seek after. They are definitive good examples.

DEDICATION

This thesis is dedicated first to my heavenly Father, the source of our possessions and to my dear parents; Mr. Joseph Riongosha and Mrs. Mary Chepkemoi for instilling in me virtues of hard work and commitment from childhood.

ABSTRACT

Universal access to financial services for a large portion of the world's population and efficient or rather effective cross-border retail payments is crucial. The traditional bank-based ecosystem is characterized by centralized control, slow transaction; high transaction costs both for local and cross-border payments. The first wave of crypto assets and cryptocurrencies, of which Bitcoin is the best known, was envisioned to address these and other issues. However, they have so far failed to provide a reliable and substitute means of payment, or store of value. They have suffered from highly volatile prices, limits to scalability, complicated user interfaces, and issues in governance and regulation, among other challenges. This research, therefore, sought to develop a model that creates a stable cryptocurrency to address the limitations of the first wave of cryptocurrency and strengthen the existing payment ecosystem by serving as a key alternative means for digital transactions and enabling growth in the digital economy. To form a basis for this study, a survey of the literature was carried out to assess the weaknesses of the existing cryptocurrency models. The results of the literature survey exposed several weaknesses including volatility which formed the center of the model design. Stability is fundamental to any payment system and at its core; the model for creating stable cryptocurrency was built on this objective to bring a greater level of stability and resilience to the payment system. Scenario-Based Design and expert focus group discussion methodologies were used to design the model. At the end of the design process, a report of the model's functional and system requirements was realized. The design was implemented using a rapid prototyping approach to realize a minimum viable product with sufficient features to evaluate the project's overall goal. The model prototype was evaluated in two phases. In the first phase, a functional testing approach was used to ascertain if the model conforms to design objectives. This was a purely technical evaluation that used test cases to see if the model requirements were attained. To ascertain the model quality, the evaluation in the second phase was done based on ISO 9126 quality framework. The ISO framework was used to design a pilot testing feedback form that 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 satisfactorily. The feedback from the pilot testing also indicated that most of the pilot testing participants were able to accomplish all the model functionalities. The majority of pilot testing participants also strongly agreed that the model satisfied all the quality attributes based on the ISO 9126 framework. The model verification and validation results showed that the model design satisfied all the intended objectives. The overall idea was therefore found to be feasible and practical. In view of the model's design philosophies, it is recommended that new opportunities for the model in the evolving payment landscape be uncovered and new design features added, tailored, and implemented to serve each unique need based on any unique circumstances.

Keywords: *Model, Stable Cryptocurrency, Fiat Currency, E-commerce*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

AMSTAR	Measurement Tool to Assess Systematic Reviews
API	Application Programming Interface
B2B	Business to Business
B2C	Business to Consumer
BIP	Bitcoin Improvement Proposal
BIS	Bank for International Settlements
BTC	Cryptocurrency Bitcoin
CASP	Critical Appraisal Skills Program (Casp) Tool
CASP	Critical Appraisal Skills Programme
CBK	The Central Bank of Kenya
CDP	Collateralized Debt Position
CSS3	Cascading Style Sheets Version 3
Dapp	Decentralized Application
DeFi	Decentralized Finance
DGX	Digix Gold Token
DLT	Distributed Ledger Technology
DYSRP	Digital Secure Remote Payments
ECC	Elliptic Curve Cryptography
EFGD	Expert Focus Group Discussion
EMV	Europay, MasterCard, and Visa
ETH	Cryptocurrency Ether
FDG	Focus Group Discussions
GDP	Gross Domestic Product
ICT	Information and Communication Technology

IEEP	Implementing Enterprise Engineering Project
ILR	Integrative Literature Review
IRL	Integrative Literature Review
KUREC	Kabarak University Research Ethics Committee
KYC	Know Your Customer
MVP	Minimum Viable Product
NACOSTI	National Commission for Science Innovation and Technology
NFC	Near Field Communication
NFIS	National Financial Inclusion Strategy
PDIOI	Planning, Designing, Implementation, Operation, and Improvement
PMGT	Perth Mint Gold Token
POC	Proof of Concept
PoP	Proof of Principle
POW	Proof of Work
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses.
PRNG	Pseudo-Random Number Generators
PTID	Participant ID
RFID	Radio Frequency Identification
RP	Rapid Prototyping
RPC	Remote Procedure Call
SBD	Scenario-Based Design
SME	Small and Mid-Size Enterprises
USD	U.S. Dollar
HCI	Human-Computer Interaction
IEEE	Institute of Electrical and Electronics Engineers

CONCEPTUAL AND OPERATIONAL DEFINITION OF TERMS

Model: Is a program that runs on a computer that creates a prototypical, or simulation, of a real-world feature, phenomenon, or event. For this study, a model was used to demonstrate and prove that is possible to come up with a model for creating a stable cryptocurrency using fiat currency.

Stable Cryptocurrency: Stable cryptocurrencies attempt to create a cryptocurrency token/ asset with a stable price. Their stability is commonly achieved by pegging the token to an asset. The study adopts this definition with cryptocurrency stability being realized by pegging its value on fiat currency.

Fiat Currency: Is government-issued money that is not backed by a physical commodity, such as gold or silver, but rather by the government that issued it. The value of fiat currency is derived from the relationship between supply and demand and the stability of the issuing government. Most modern paper currencies are fiat currencies, including the Kenyan Shilling, the U.S. dollar, the Euro, and other major global currencies. The study adopts this definition by referring to the Kenya shilling (as fiat currency).

Global E-commerce: Is the buying and selling of goods or services over the internet across geopolitical borders from a company's country of origin. The study adopts this definition to describe the envisioned capabilities for the created cryptocurrency to reduce the cost and improve the efficiency of cross-border payments and facilitate diaspora remittances

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 industry 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. For this study, the developed model was deployed to the blockchain network to demonstrate how to keep track of the transactions.

Ethers: Are 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.

Smart Contract: 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. The study adopts this definition in the operationalization of the model design element.

CHAPTER ONE

INTRODUCTION

This Chapter of the research thesis provides a background of the fundamental concepts including; the probleminforming the proposed study and the justification for the necessity to provide a stable cryptocurrency**.** It further continues to outline the research objectives and the research questions as well as the scope, assumptions, and significance of the study.

1.1 Background of the Study

The rapid growth of the Internet and digitization of enterprises has significantly affected all economies across the world. The monetary sector has been directly influenced by technology due to the striking growth of e-commerce and e-payments. The traditional bank-based ecosystem is being disrupted by the digitization of financial services and the emergence of cryptocurrencies. In a recent survey carried out by Sitienei et al (2020), banks and financial services were ranked the most affected by rapid technological advancement. They were also projected to uphold the top rank for five years since the time of the study (Sitienei et al., 2020).

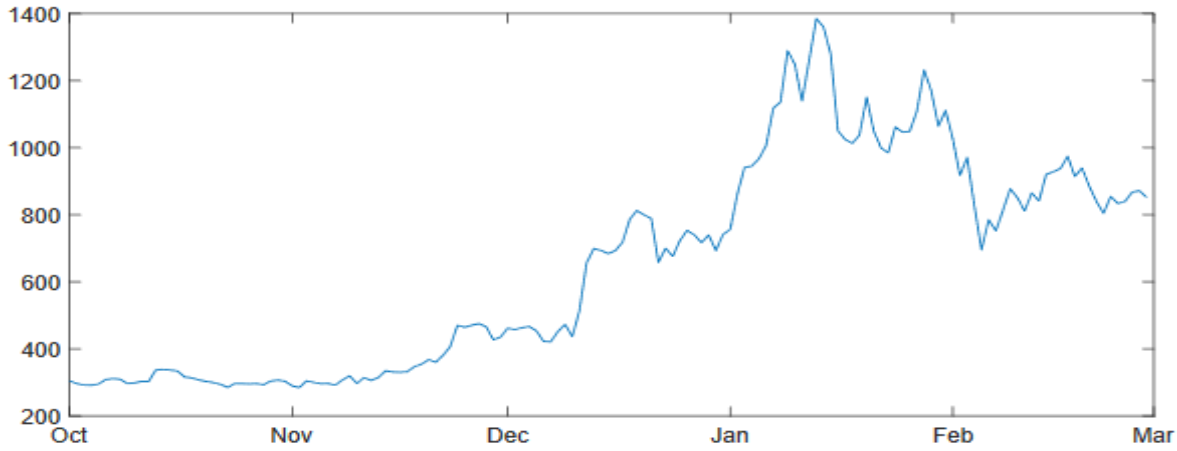
Despite significant improvements in recent years, research carried out by Bayram (2020) on the globalization of financial services and cross-border banking performance indicate that the current payment systems still have two foremost deficiencies: first, lack of universal access to financial services for a large share of the world's population and secondly it indicated that there are inefficient cross-border retail payments.

Cryptocurrency technology and crypto tokens were originally envisioned to overcome these problems due to the ground-breaking potential of the underlying blockchain as well as the distributed ledger technology (DLT) (Bayram, 2020). However, cryptocurrency prices are highly volatile, responding strongly to global events and speculative concerns about the cryptocurrency

market. As shown in Figure 1 below, the price of the Ether coin compared to U.S. dollars from Oct. 2017 to March 2018 was taken. During this period, ETHhad an annualized return volatility of 120% in relation to USD. This shows high volatility for a medium of exchange or a store of value. It also turns cryptocurrencies into a highly risky asset class for certain investors and those involved in illegal activities, rather than a method of payment.

Figure 1

ETH/USD Price From 1 Oct 2017 to 28 Feb 2018



According to Moin's et al (2020), research on Financial Cryptography, for a token to effectively function as currency, its purchasing power against goods and services must remain constant over the short to medium term. In this regard, there is a need to devise a framework to minimize the market volatility of cryptocurrencies while maintaining the present features of current crypto-technology. This would allow users to take advantage of blockchains' huge potential and disruptive impact, without the risks that come due to the price volatility of the cryptocurrency

Blockchain technology refers to the processes and related technologies that allow nodes in a network to securely propose, validate, and cross-authenticate historical records. The network's nodes synchronize and store state changes and updates in a distributed ledger (Kannengießer et al, 2020). In the context of payment, clearing, and settlement; Blockchain-based transactions enable

users to carry out transactions without relying on a central authority to maintain a single copy of the ledger (Xu et al, 2019). In the Validation of a blockchain-based process, nodes identify state changes that are consistent according to the rules of the arrangement. This ensures that the assets are available to the originator. Further, the originator and the beneficiary are entitled to interchange the assets. To efficiently do so, every node needs to depend on a record of previous parent states, either as a "last agreed state" or as a "chain of previous states" (Kannengießer, 2020). With these features, blockchain and cryptocurrencies have attracted noteworthy interest. As a result, over the past few years, transaction services have realized an outstanding transformation through the introduction of new payment methods, platforms, and interfaces with Bitcoin and other cryptocurrencies' digital infrastructure at its core.

In research to explore the universal spread and growth of Bitcoin as a system and infrastructure enabling the use of Bitcoins by Bullmann et al, (2019), it was found that Cryptocurrencies are thriving. A decade since the discovery of Bitcoin, the current total market capitalization of the entire cryptocurrency market is $25.61 billion (Coinmarketcap, 2021). To put this in perspective, there is currently USD 1,759.8 billion and 30.4 billion Euros in circulation (U.S federal reserves, 2020: European central bank, 2020). As of November 2019, Bitcoin was the world's sixth-largest currency in circulation. According to (Zhang & Gregoriou, 2020), the average daily exchange of digital tokens and cryptocurrencies has surpassed one percent of exchange in foreign exchange markets. Over the last five years, Bitcoin transactions and exclusive accounts have increased at a rate of nearly 60% per year (Huang et al, 2020).

According to Danielkenz (2020), Africa is the ideal breeding ground for the crypto ecosystem. It attributed the possibility of widespread cryptocurrency adoption to the current financial setup. It pointed out that the presents many under-banked persons and well-established financial institutions

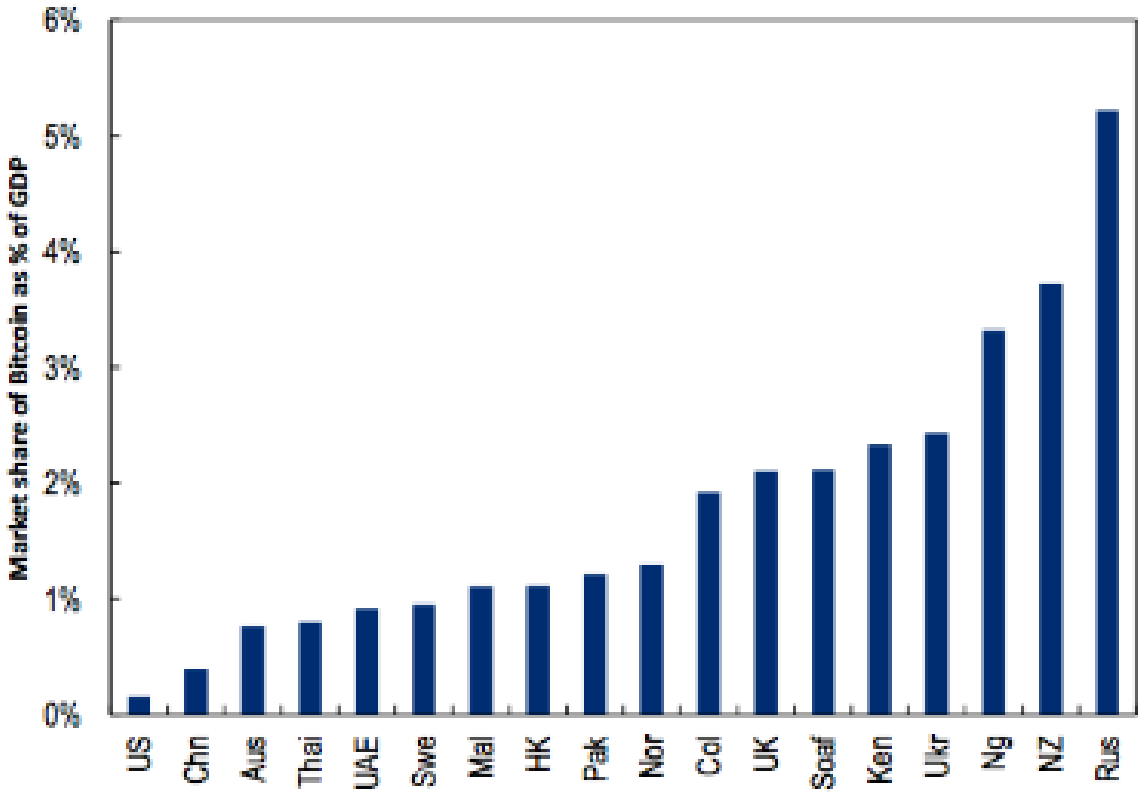
who have not penetrated deep into the fabric of African society as the possible reasons to stimulate high adoption. Blockchain Association of Kenya (2019) estimates that Bitcoin transactions are worth over $1.5million per year. This association is actively working to educate the country on the benefits of using cryptocurrencies and blockchain.

Investors and other important players observing the crypto market in Africa for example Sungroowmall and BlockBankare observing Kenya and other developing countries in Africa. Sungroowmall is ranked as the largest decentralized web 3.0 cryptocurrency marketplaces globally and is looking to expand into Kenya (CryptoGuru, 2019). It provides a platform for buyers and sellers to find trade opportunities and promote their businesses online. The platform has been functional in Nigeria collecting a large number of users. BlockBank is a United Kingdom-based blockchain bank that was set to open an office in Nairobi to attract five million Kenyan customers (Ngunjiri, 2018). This imminent opening would increase the number of cryptocurrency traders in the country and the need for integration with the present payment methods. The lender uses distributed ledger technology (DLT) and targets small and medium enterprises (SMEs), commercial entities, and international commercial financial markets.

According to a report by cnbcafrica (2020), the African countries namely; Nigeria, Kenya, and South Africa are ranked among the top ten countries in cryptocurrency adoption. Kenyans have continued trading and holding cryptocurrencies and the country is now estimated to hold more than KES 163 billion worth of Bitcoin, equating to 2.3% of Kenya's GDP. (Schizas et al, 2019). Figure 2 below shows Kenya's Bitcoin holding in relation to GDP compared to other international markets. The observation from this discussion shows that cryptocurrencies are being adopted rapidly and broadly.

Figure 2

Kenya's Bitcoin Holding in Relation to GDP Compared to Other International Markets



The general features of DLT increase the efficiency and transparency of collaborations between individuals and/or organizations (within or cross-borders). This is based on inherent qualities such as tamper resistance and censorship resistance and democratization of data (Li et al, 2019). The cryptocurrency core functions in a blockchain platform include; being a unit of account, medium of exchange, store of value, and a transaction validation fee (Zhang & Gregoriou, 2020). The first function identifies that cryptocurrency is used as a unit of measurement. The second function expresses it as an instrument for exchanging assets between agents within the blockchain platform. The third function is an extension of the second function due to time. Storing value implies someone trading his supply of goods or services for money today, hoping he/she can exchange money back for other goods or services in a sufficient long-run period. The last function refers to

the cost necessary to perform a transaction on the blockchain platform (Helo & Hao, 2019). These, therefore, illustrate that cryptocurrency is an important element in the blockchain ecosystem.

1.2 Statement of the Problem

Cross-border trade is vital for all economies. Globalization of financial services and cross-border banking performance however shows that current payment systems still have two major flaws: lack of universal access to financial services for a large portion of the world's population and inefficient cross-border retail payments (Bayram, 2020). The introduction of digital ledger technology and cryptocurrency was intended to address the problems associated with current payment systems by introducing a more universal and secure electronic payment method for cross-border digital payment. However, cryptocurrencies have been hampered by short-term extreme price volatility. This is because there are no mechanisms in place to dynamically adjust supply to changing demand. For instance, Bitcoin experienced a price surge in 2017 that brought its value close to $20,000. It, on the other hand, experienced a series of crashes throughout 2018, causing its value to fall below $4,000 (Lahmiri et al, 20).This indicates that the price of Bitcoin is highly volatile and susceptible to reacting strongly to cryptocurrency price volatility drivers.

Several cryptocurrencies and Tokens already exist, and new cryptocurrencies are constantly being introduced in an attempt to support and improve the blockchain and crypto technology ecosystem. Furthermore, at the time of this research, the total market capitalization of all coins in the world was approximately $361,954,584,478. (TradingView, 2021). With so many cryptocurrencies and so much market capital, this research found that there was a need to address price volatility issues as a contribution toward improving this technology.

Consider the following scenario of two types of a single unit of currency;

"*One Kenya shilling (fiat currency) would allow one to purchase one Kinder Joy today and possibly in a year, but purchasing that same Kinder Joy using Bitcoins, X BTCs value would be vastly different from now due to Bitcoin's volatile value. It's possible that it won't get you any Kinder Joys next year, or that it will get you 100 Kinder Joys"*

Stabilized cryptocurrency becomes perhaps the most significant element in this scenario. The projected Stable cryptocurrency is a form of crypto-asset with consistent and predictable values. This would leverage the field of business and information technology to bridge the gap of strategic implementation of information technology systems in business to realize stable and universal access to financial services for the larger world's population and efficient cross-border retail online and offline payments methods.

1.3 Objectives of the Study

1.3.1 General Objective of the Study

The primary concern of the study was to develop a model for creating stabile cryptocurrency using fiat currency to enhance global electronic commerce.

1.3.2 Objectives of the Study

i) To explore the weakness of existing Cryptocurrency models Used in E-commerce.

ii) To design a stabilized cryptocurrency model for global electronic commerce.

iii) To implement the stabilized cryptocurrency model design for global electronic commerce

iv) To evaluate the model for creating stable cryptocurrency global electronic commerce

1.4 Research Questions

The research seeks to answer the following questions;

i) What are the weaknesses of the existing Cryptocurrency models Used in E-commerce?

ii) How can a model for creating a stable cryptocurrency using fiat currency be designed?

iii) How can a model design for creating a stable cryptocurrency be implemented?

iv) What is the performance of the implemented model prototype?

1.5 Justification of the Study

The proposed model for creating a stable cryptocurrency using fiat currency for global electronic commerce stands to significantly benefit both the financial and cryptocurrency industry. The model is meant to reduce crypto-asset price volatility while maintaining the features of the present crypto-technology while allowing users to take advantage of DLT's huge potential and disruptive impact.

The current cryptocurrencies have been discovered to have high price volatility, making them poor mediums of exchange or stores of value. As a result, they serve as a highly speculative asset class for certain investors and those engaging in illegal activities, rather than promoting the financial industry.

The model design feature of using peer-to-peer transactions and the cryptographic nature of transaction records provide potential opportunities in the financial industry. It offers a possible solution to the current problems of a significant portion of the world's population lacking universal access to financial services and inefficient cross-border retail payments. It emphasizes realizingthe stability and efficiency of payment and settlement systems, along with universal access, instant payment capability, and interoperability (Bouri et al, 2019). This, therefore, is projected to provide

a digital currency alternative to cash that would support the payment system at a lowcost, and facilitate secure access to goods or services in a peer-to-peer trading ecosystem.

In the present evolving payment landscape, this model intends to contribute to digital payment and further enhance the digital economy while supporting sovereignty. Further, it provides an opportunity for digitalization and to contribute as an alternative in the countries with the prospect of declining use of cash during the coronavirus (COVID-19) pandemic.

Integration of cryptocurrency and the underlying DLT technology is critical in today's data-driven industries and economies, where data is the most fundamental and core aspect. The DTL consensus-enabled comprehensive, secure, and unalterable data repository can streamline the ever-increasing transaction volumes and multi-party verification processes that are needed. This reduces the burden of document assembly between parties and saves time by consolidating document storage, reducing the risk of data loss and missing documents. This, therefore, requires the current cryptocurrency to be improved and its present challenges including volatility must be addressed.

In the countries that highly depend on diaspora remittances as the key source of foreign exchange such as those in sub-Saharan Africa, this model would provide a secure and cost-effective process for remittances and ultimately boost remittance flows. It would also reduce the number of remittances flowing through informal channels as the cost of remittance will be significantly low. This model will make remittances easier, faster, and cheaper.

This model will also contribute significantly to the efforts of the cashless society of Kenya in enhancing the digital economy. This involves the development and modernization of payment systems to drive economic growth and ensure the provision of efficient payment options while driving financial inclusion and economic development

1.6 Scope of the Study

This study focused on the development of an application model for creating stablecryptocurrency using fiat currency for e-commerce. Through this research, the researcher put thoughts and ideas about the need, and how to design and implement a firm cryptocurrency for local and cross-border payment. The participants involved in the study were blockchain experts drawn from blockchain-based companies and associations. They were involved in reviewing the cryptocurrency weaknesses derived from the integrative literature review to ensure atomicity and define the model requirements (majorly functional requirements). The prototype developed served only as a proof of concept and was a complete commercially applicable model. The evaluation of the model was done from a technical perspective based on the initial objectives and system requirements.

This research addressed the gap that views cryptocurrency as a poor medium of exchange and a worse unit of account due to high volatility. This enables blockchain users to take full advantage of DLT's huge potential and disruptive impact. Thereby, through this research, we sought to offer a novel and broader account for the growth of this type of financial technology.

1.7 Limitations of the Study

Although the general objective of this research was to realize a model for creating a stable cryptocurrency using fiat currency for e-commerce, the blockchain main network requires a real value for transaction validation. To overcome this limitation, this study was limited to studying and implementing blockchain and cryptocurrency technologies in an Ethereum virtual machine platform. The Ethereum Virtual Machine platform supports the creation of decentralized applications (DApps) and manages accounts and smart contracts.

1.8 Assumptions of the Study

The development of the proposed model assumed that during the model development, testing, and verification, faucet lenders for test ethers would increase the lending amount per account. However, this was not the case and the creation of more than one account was used to get the test ethers.

The study also assumed that all the participants were knowledgeable in blockchain and cryptocurrency technology and intelligent enough to contribute to discussions appropriately. Fortunately, this was the case and there was no training undertaken and questions were answered with required honesty and integrity.

1.9 Structure of the Thesis

This thesis is structured as follows: Chapter One presents the introduction of the study including the background and statement of the problem, the purpose of the study, the research objectives, and research questions, contribution of the study, justification as well as the delimitation, assumptions and the limitations of the study.

Chapter Two presents a detailed literature review of existing knowledge related to the study. Existing gaps are also highlighted in this chapter.

Chapter Three presents the methodologies applied in this study. The philosophical theory and the design approach supporting this study are discussed. Besides, the methods used in the research include integrative literature review (ILR), Focus group discussions (FGD), scenario-based design (SBD), Functional testing using test cases, and pilot testing.

Chapter Four presents the survey results. The findings of the study including the analysis and discussion of the results are presented in this chapter. Further, the model design, implementation, and evaluation are also presented in this chapter.

Chapter Five presents the general conclusion of the study presented in this thesis and proposes research directions that may be investigated in future work.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter presents a review of the critical points of current knowledge, among them being substantive findings of the literature related to the study. These include literature related to the existing model that seeks to stabilize cryptocurrencies and various approaches used for their implementation. The conceptual framework and the model architecture for the envisioned study will also be presented and discussed.

2.1 An Overview of Electronic Commerce

Electronic commerce (E-commerce) refers to the buying and selling of goods or services via the internet, and the transfer of currency and data to execute these transactions as shown in Figure 3 (Sanyala & Hisamb, 2019). It could also be defined as a commercial transaction that is facilitated through the internet platform. Since the advent of the first e-commerce transaction in 1994, it has evolved to make purchases easier to discover and purchase through online retailers and marketplaces (Kumar, 2019).

In a study by Arlott et al (2019), Independent service providers, small businesses, and large corporations have all significantly benefited from e-commerce. This has enabled the said businesses to trade their products, goods, and services at a measure that was not possible with brick-and-mortar business setup. E-commerce has helped businesses establish a wider market presence by providing cheaper and more efficient distribution channels for their products or services. In research to forecast the growth in the percentage of E-Commerce sales from 2017 to 2023, it found that Global retail e-commerce sales are projected to reach $27 trillion by 2021 (Yanyan, 2018).

The rise in the use of mobile devices globally, the data-driven nature of the present economy, improved consumer experience, and the low cost of running an online business has contributed to the growth of E-Commerce (Tran, 2020). Through mobile devices, individuals are buying and selling over the Internet more flexibly. Several FinTech-based companies are transforming payment methods, making them secure and simple to effect mobile-based transactions. E-commerce businesses rely on these payment systems and integrate them into their mobile-based applications.

The statistical and arithmetic observations gathered by E-Commerce businesses have also contributed to the development of E-business. In the Business-to-Consumer model, for instance, online-based businesses track consumer preferences and make significant observations (Hansson & Manfredsson, 2020). These observations are then integrated into retail models for seamless future purposes, ensuring that e-commerce sales soar globally. Consumers are usually in search of product offers at very affordable or discount prices. As pointed out in the research paper "Barriers and drivers of multi-channel e-commerce" by (Acquila-Natale et al, 2019), the low cost of running an E-commerce business also influences growth. It indicates that it is relatively cheaper to establish an online store than a physical one as E-commerce eliminates the need to build physical stores in which products are cataloged.

In essence, running e-commerce allows the selling of goods and services on a global scale. It uses a single platform for anyone, anywhere online with an online-based store, online market places, or social media. It also improves marketing strategies through the use of built-in tools that could create, execute, and analyze campaigns on social media (Natea & Kaliyaperumal, 2020). Above all, e-commerce platforms through a single dashboard help in managing orders, shipping, and payments, therefore, enhancing business manageability.

Although the above drivers and motivation of e-commerce have been appreciated by several scholars, the question this research asks is how the potential of cryptocurrency and blockchain marketplace be integratedinto e-commerce? Given the continued advances in technology worldwide, how can we engage in cross-border e-commerce to achieve the transformation of convenience stores into huge multinational organizations? How could every business now address the online demand of customers at home and abroad through a transparent and sustainable online environment to achieve the full potential of cross-border e-commerce?

Figure 3

E- Commerce Diagram

2.2 Electronic Payment Systems for E-commerce

Any money transaction needs at least two parties (a sender and a receiver). The system that is required to carry out the transaction is called a payment system. This system is built with the central bank, commercial bank, payment service providers and mobile money agents, payment gateways, payment aggregator, and/or payment methods to facilitate the transfer of money between a payer and payee (Pazarbasioglu et al, 2020). The inclusion of all these mechanisms forms a payment ecosystem. The payment ecosystem is not a static system; it changes whenever technology or culture is changed or thrives.

In an e-commerce environment, a payment system requires a currency of the transaction. There are two main currencies of transaction in circulation today namely fiat currency and cryptocurrency. Cryptocurrency is a private decentralized network-based currency (Hossain et al, (2020). Cryptocurrencies are mainly symbolic currency that is used in the business virtual world which works on the cryptographic principle (Umar & Gubareva, 2020). They exist as a collection of programming codes that also provide high security and usability than many existing currencies. On the other hand, fiat currency is the physical and digital form of currency that has been set up as money, often by government regulations. The value of the Fiat currency is government-controlled (Dong & Zheli, 2020).

2.2.1 Payment System in E-CommerceBased on Fiat Currency

The Era of Information and Communication Technology (ICT) and digital innovation lead to dynamic changes in the commercial environment, where business transactions continue to shift from cash-based transactions to electronic-based transactions. E-based payments can be understood as a payment mechanism using electronic media that does not involve cash (Jeon

&Stita, 2020). E-payment is an important aspect of e-commerce. Some of the e-commerce payment methods presently in use include;

a) PayPal

PayPal is an online payment method that aimed to remove the need of using credit card information to make any payment and serves as an electronic alternative to traditional paper methods like checks and money orders. Since its invention, PayPal has rapidly grown in popularity in the world. In 2019, 37.3 million new active Paypal accounts were created raising the total active accounts to 305 million (Hossain et al, 2019). In the third quarter of 2020, PayPal's net payment volume amounted to around 246.7 billion U.S. dollars, representing a 38 percent year-on-year growth (statista, 2020). Overtime PayPal has become an essential method for payment all over the world. It charges a fee in exchange for benefits such as one-click transactions and password memory. It is simple to set up, use, and navigate through the Paypal system and convenient to manage the transactions as compared to the conventional merchant accounts, which were previously used. It does not limit transfer size nor need any account maintenance fee thus contributing to the business' flexibility for sales and growth. PayPal's transaction fees however are quite higher than those of most traditional merchant accounts. It has a transaction rate of 2.9% per transaction (Hossain et al, 2020). It also suffers from centralized control issues, which are the most common problems that its users face, because PayPal has the right and may frequently freeze and take over the money in your seller account (without first contacting you) if a buyer raises a dispute or suspicious activity is detected. Furthermore, once PayPal resolves a buyer-initiated dispute, the seller cannot appeal the decision. There's no chance of a third-party jury.

b) Apple Pay

Apple Pay is a mobile payment digital wallet service that is only supported by iOS devices like iPhone, Apple Watch, iPad (Olenina & Zipunnikova, 2017), and Mac. The main transaction is a point-of-sale terminal by which a credit card, debit card, chip, and PIN for the transaction. In Apple Pay, online-based payments are simple for the E-customer because credit cards authenticated with Touch ID use the information that is stored in the participating apps which the Apple API already accepted. It is also used for Digital Secure Remote Payments (DYSRP) and also for contact-less Europay, MasterCard, and Visa (EMV) payments at the point of sale. Apple Pay supports secure transactions in several aspects. The user authentication involves the use of Bio-metric Fingerprint verification which is Touch Id. This ensures user security and also prevents fraud interruption. Data Protection is provided by a unique derived key, the apple pay applets, token Pan which is the account ID, and certified issuer payment applets all are stored securely in a Secure Element (Hossain et al, 2020). Apple pay users do not have any extra credit card transaction fees. However, to enjoy the apple pay payment services users are required to have an iPhone 6. Its transaction speed is also low and API support is underdeveloped. Apple company which is a third-party act as a central point and maintain all the incoming and outgoing money transaction between any e-commerce organization or those types of organization that supports online transaction.

c) Google Pay

Google pay or Google Wallet is a peer-to-peer payment service developed by Google. With this service, users can access their online accounts through their debit cards. User requirements for a transaction are personal email or a number (O'leary et al, 2019). This method was designed to enable customers to pay with their Near Field Communication (NFC) enabled Android devices using tap-to-pay or in-app. Near Field Communication (NFC) is a standard that uses a specific

frequency of Radio Frequency Identification (RFID) that allows communication between active readers, passive tags, and peer-to-peer active readers. An NFC-enabled phone can read the tag, receive and send data to another NFC-enabled phone. Google pay has faster payment with a tap-to-pay feature and offers API to third-party developers to integrate with their applications. It however uses telemetry to collect information like location and time and it also requires Android device 4.4 (KitKat) and above (Caddy et al, 2020).

d) Skrill

Skrill is a popular mobile payment operator and an online digital wallet provider which offers a range of online payment and money transfer services. Skrill users upload money to their Skrill wallet using various payment options, including by card, bank transfer, and several alternative payment methods (Hossain et al, 2020). Skrill also offers cross-border payments via its remittance service, Skrill Money Transfer. The service enables customers to send money to a bank account overseas using their bank cards. Skrill platform transaction costs for money withdrawal are minimal with central control and it is much faster to withdraw funds as compared to its competitors. Skrill is an effective and easy method of transferring large amounts of money in a Casino, suppose you have a verified account. Skrill however suffers from bureaucratic leadership and transparency issues that result from its centralized nature as compared to blockchain-based payments that can go for a complete decentralized network where there is no need for a centralized authority, improving the system's transparency. It is also hard to trace items that can lead to multiple problems, including theft, counterfeiting, and loss of goods (Raj et al, 2020).

e) Amazon Pay

Amazon Pay is an online payment platform that can help streamline customers' order management and payment experience (Lee et al, 2020). It allows users with existing Amazon accounts to make purchases on thousands of their favorite sites around the web without the need for platform setup. The presents of intermediaries in amazon pay, however, increase the transaction fees and delay the transaction process.

f) Klarna

Klarna is an online payment service platform that gives users a seamless, intuitive, and enabling shopping experience. It is an example of a 'buy now pay later' instant financing platform, that offers customers a way to spread the cost of their purchase or simply pay for their items at a later date, rather than pay in full upfront. Although klarna offers credit options with an appeal to buy now and pay later option, its transaction costs are high (2.95%). The centralized nature of its operation also reduces transparency and security (Hossain et al, 2020).

2.2.2 Cryptocurrencies Used in E-Commerce

Smith & Kumar (2018) define a cryptocurrency as a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Cryptocurrencies are decentralized networks based on distributed ledger technology (blockchain technology). It uses consensus mechanisms that ensure that all participants agree about the ownership rights to the virtual currency units. This consensus mechanism is the core innovation of the Bitcoin system and allows consensus to be reached on a larger scale and in the absence of any personal relations. Cryptocurrency maintains its integrity through peer-to-peer networking and cryptography. Its inventors introduced Bitcoin in an attempt to move away from the trust-based model of traditional currencies and create a secure system based on cryptographic proof. Although the market

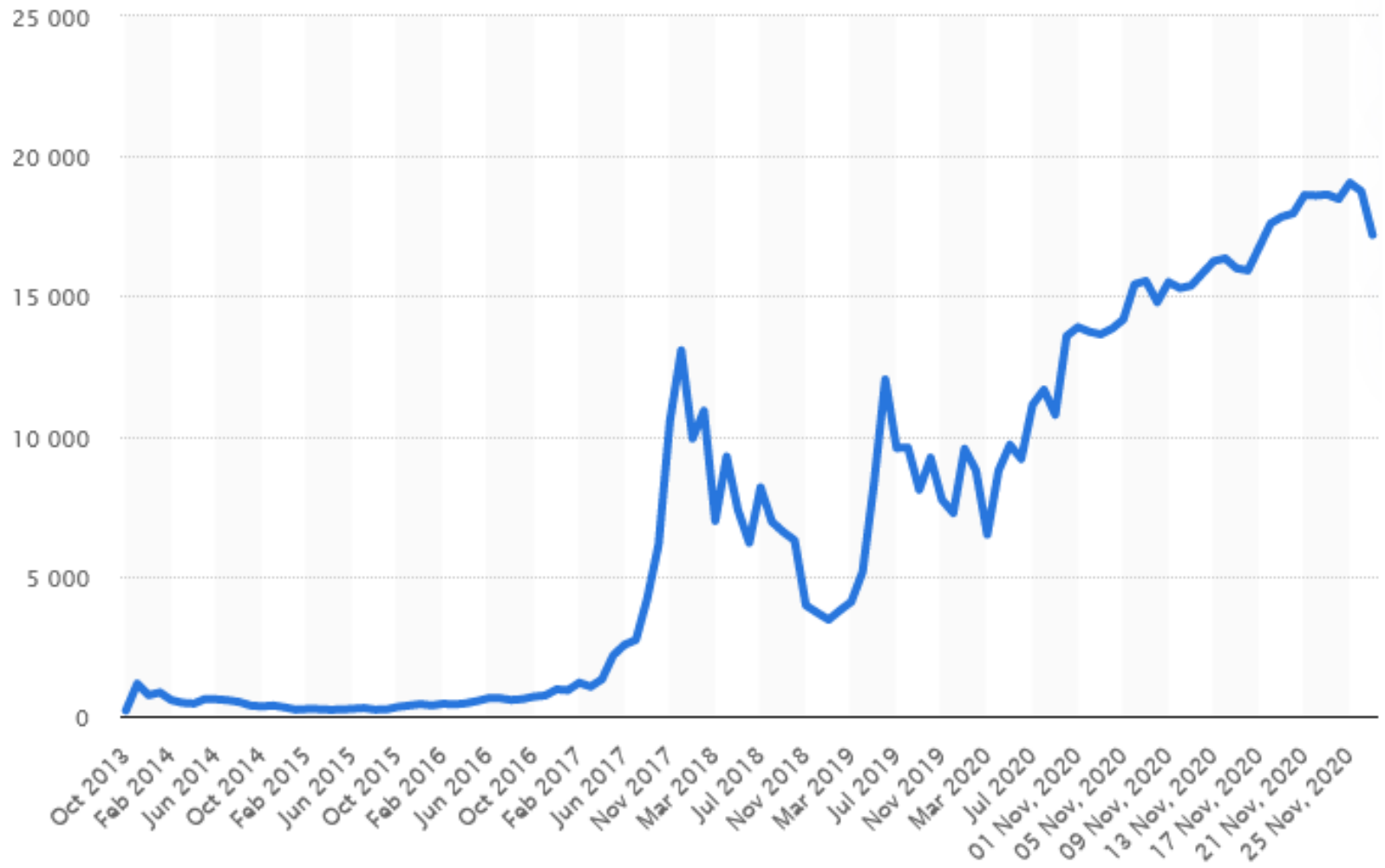
capitalization of all cryptocurrencies has grown in value by more than 1000 percent at certain points over the past year, research shows that it has also seen significant plunges in value (Qureshi et al, 2020). Statista (2020) illustrates how cryptocurrency has had a volatile trading history since its inception in 2008/2009 in Figure 1.

a) Bitcoin

Bitcoin (BTC) is the original blockchain digital virtual and it remains the go-to leader in the space. As of this research, the market capitalization of the Bitcoin currency is more than **$** 337.20 billion, with a price per coin of more than **$** 18,517.79 and 18,558,137 BTC circulating supply (coinMarketCap, 2020). Statista (2020) indicates that Bitcoin held a 66 percent share of the total cryptocurrency market in 2020. Despite many indications that bitcoin is more widely used as a currency, Sharma et al(2016) however, argue that bitcoin price volatility is many times larger than that of stocks, bonds, hard currencies, and commodities. Further, its lack of essential value and regulation suggests different characteristics than many traditional assets. The first Bitcoin price hike happened in 2013 when a single Bitcoin was trading at 1,124 U.S. dollars in November (statista, 2020). As shown the figure 4 as well, four years later Bitcoin experienced a meteoric rise and reached record highs, with some exchanges having the price of a single Bitcoin at about 20,000 U.S. dollars in late 2017.

Figure 4

Bitcoin Price from October 2013 to November 27, 2020

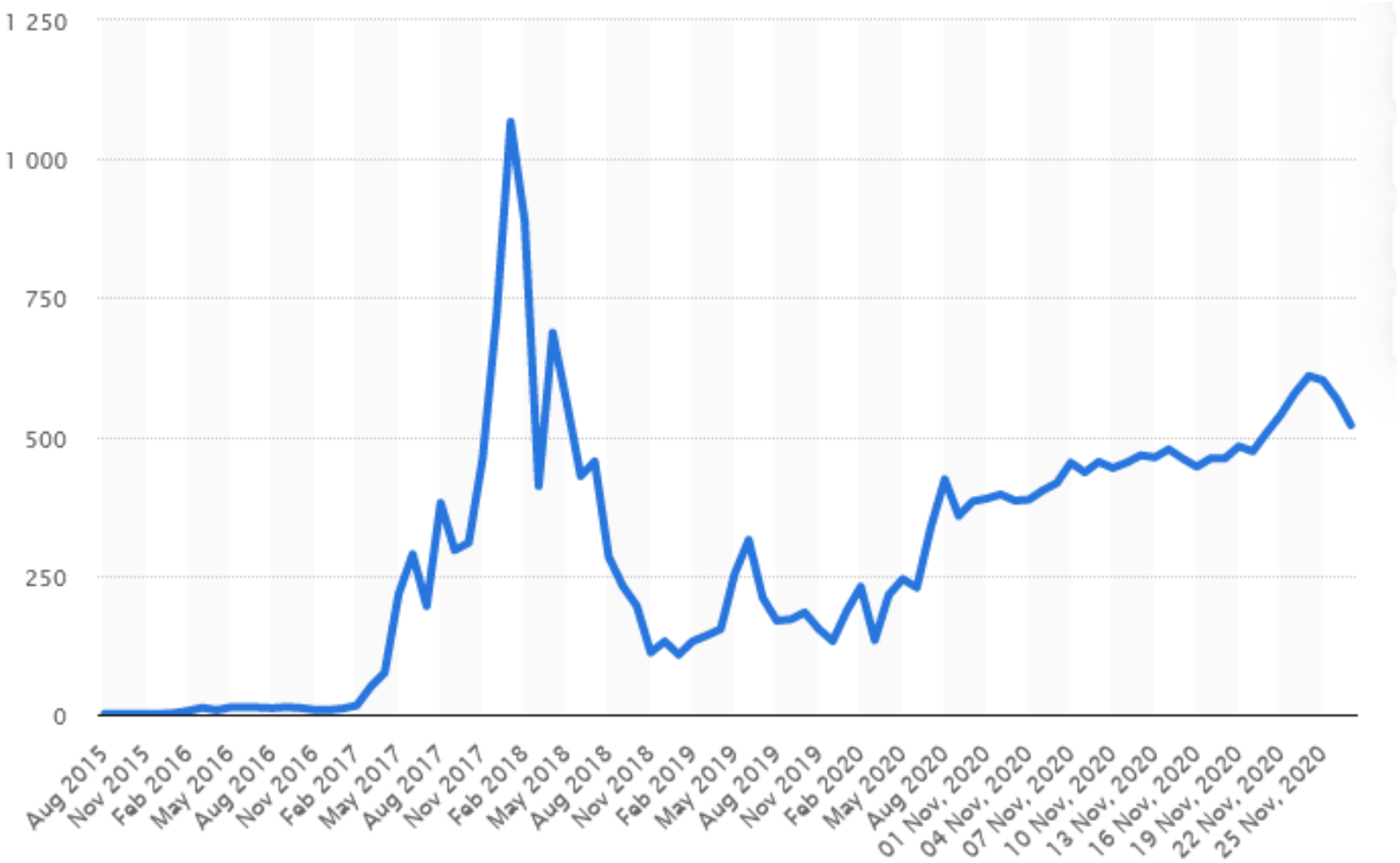


b) Ethereum

According to Kondo et al, (2020), ETH (Ethereum) is a distributed open-source blockchain system that features its cryptocurrency, Ether. ETH works as a platform and a host for numerous other tokens and cryptocurrencies, as well as for the accomplishment of decentralized smart contracts. Smart contracts are self-executing programs that automatically execute the actions necessary to fulfill an agreement between parties on the internet. They were designed to reduce the need for trusted intermediates between contractors, thus reducing transaction costs while also increasing transaction reliability. ETH was first described in a 2013 whitepaper by Vitalik. At the time of this research, the ETH price is USD 582.42 with a market cap of USD 66,184,795,233, and also with the 24-hour trading volume of ETH is $19,087,917,197(CoinMarketCap, 2020). Despite the growth and numerous adoptions of Ethereum, statista (2020) describes Ethereum value from August 2015 to November 27, 2020, showing high price volatility. In January 2018, the price of ETH was USD 1067 and in January 2019, ETH was trading at USD 108 as shown in the figure below. This renders Ethereum highly volatile and a poor medium of exchange or a store of value.

Figure 5

Ethereum Value from August 2015 to November 27, 2020



2.3 Volatility in Cryptocurrencies

Volatility describes the extent to which an asset's price fluctuates over time (Olkhov, 2020). Based on the historical price charts, cryptocurrency values have been historically quite volatile. In three months from October 2017 to January 2018, for instance, the volatility of the price of bitcoin reached nearly 8% (Moratis, 2021). This is more than twice the volatility of bitcoin in the thirty days ending January 15, 2020 (Meegan, 2021). According to Möser and Böhme (2017), in 2016, the price of bitcoin rose by 125% and in 2017 the price rose again, this time by more than 2,000%.

2.3.1 Causes of Cryptocurrency Price Volatility

Price fluctuations in the crypto asset spot rate on cryptocurrency exchanges are driven by many factors. According to (Katsiampa, 2019) one of the contributing factors tothe price volatility of cryptocurrency is the fact that the cryptocurrency market is still small and emerging compared to fiat currency and gold. The study also pointed out that the relatively small market size means that smaller forces can have a larger effect on price. However, the fact that the cryptocurrency market is still developing also means there are many opportunities to hit it with a new and exciting project and this calls for innovation to reduce volatility.

The lack of governance of cryptocurrency is another contributing factor to price volatility as presented by (Henderson & Raskin, 2019). Most cryptocurrencies are purely digital assets and aren’t backed by anything physical like a currency or commodity and there are no governments to enforce their use as a currency (Henderson & Raskin, 2019). This means that cryptocurrency value is backed entirely by faith and their prices are set by the laws of supply and demand.

Blockchain and other alternative crypto technologies are also still in their early stages of development. It is barely a decade since the idea of cryptography-based decentralized currencies was published in the Bitcoin whitepaper. Yen and Cheng (2021) indicate that it will be a while

before the market matures, as many innovations to improve it will sprout. Above all, the present crypto market lacks Regulation and Institutional Capital. Governments across the world are scrambling to put in place proper regulatory frameworks on cryptos (e.g. blockchain society of Kenya). The absence of regulatory oversight results in market manipulation which introduces volatility. This, in turn, discourages institutional investment in the market.

In addition, speculation is another contributing factor to price volatility as stated by Corbet et al, (2021) study. The study points out that due to a lack of intrinsic value, investors depend on speculation that the price of different cryptocurrencies will either go up or down by buying and selling cryptocurrencies. This makes cryptocurrencies susceptible to speculative bubbles fueled by irrational speculative activity.It is the volatility of the cryptocurrency market that lures speculative traders looking to make big money by guessing the swings. Many investors are constantly trying to guess the ups and downswings of the cryptocurrency market. These speculative bets cause even more volatility in an already choppy market.

As cryptocurrency is a small market of digital assets with tons of speculation, the media stories surrounding the cryptocurrency market have an outsized and massive impact on where the prices go (Bouri et al, 2019). Speculators and investors are constantly eyeing the headlines for the next big news story that will launch or crash the market. When something does emerge, everyone knows it's a race to buy or sell and the fastest will profit the most, while the slowest will lose the most.

2.4 Suggested Cryptocurrency Stabilization Mechanisms

The following approaches to the realization of price stabilization of crypto assets have been attempted according to Dell'Erba (2019).

2.4.1 Crypto-Backed Coins

The crypto-backed mechanism has other cryptocurrencies locked up as collateral. It uses a 'security pledge' to compensate for the volatility of the cryptocurrency which is being used as collateral. This will allow a higher level of decentralization, easy, and quick transactions because it is fully blockchain-based. It does not require a trusted custodian or external auditing while maintaining high liquidity. However, the system is more complex and the pledge system has less promise of stability in the case of a huge spike increase or decrease of the collateralized stablecoin (Moin et al., 2020) The stablecoin is dependent on the collateralized cryptocurrency.

2.4.2 Gold-Pegged Coins

Gold-pegged mechanism associates the designed crypto-asset with the value of a particular unit of gold. Gold-backed cryptocurrencies have the potential to address regulatory and policy concerns by decreasing the volatility of cryptocurrency prices and facilitating a broader cryptocurrency adoption (Jalan et al, 2020).The volatility of these coins will greatly depend on the value of the peg (gold) increasing the susceptibility to volatility transmitted from gold markets.Gold-backed tokens can also be used as collateral for peer-to-peer lending since this information would be safely and securely stored on the Blockchain.

2.4.3 Non-Collateralized Coins

This mechanism relies on an algorithm-generated mechanically which can change the supply volume if needs be to maintain the token's price which is pegged to an asset (Lee, 2020). It relies on smart contracts to sell tokens if the price falls below the peg or to supply tokens to the market if the value increases. In this way, the token remains stable and hold its peg. Since it does not rely on collateral, any central entities are independent and there is fundamentally no need for collateral, which avoids many issues related to centralization; Smart contracts put in place allow for more

trust since the peg is tied to an algorithm and not collateral. However, the mechanisms are far more complex than collateralized stablecoins and the nature of the system means there is a constant demand for the stablecoin to succeed which is not always guaranteed.

2.4.4 Oil-Backed Cryptocurrency

Oil-backed cryptocurrency is backed by the tangible asset of oil and sometimes gas reserves. This essentially means tokenizing barrels of oil held in reserve to give increased credibility and price stability to the cryptocurrency. The oil backing the currency is meant to counter volatility. Crude oil is the most exported product in the world. In 2017, crude oil shipments were worth $841.1 billion (just one year after the market collapse of 2016) (Manzoor& Norouzi 2020). The market is pretty stable, and that could make any oil-backed cryptocurrency a relatively stable option.

2.5 Existing Models that Have Attempted to Realize Cryptocurrency Value Stability

This section presents a review of the existing models that have attempted to use the approaches to realize a stable cryptocurrency discussed in section 2.4 above. To appreciate the need for the proposed model, the existing real-world alternative needs to exhibit inefficiencies in their use cases. The selection and review of the existing cryptocurrencies in this research were guided by the following parameters; model popularity (number of users), market capital, collateralized or non-collateralized. The parameters were obtained from a framework presented by Templier et al, (2015) in a study titled framework for guiding and evaluating literature reviews. The analysis and results are presented in Table1.

2.5.1 Digix Gold Tokens (DGX)

DGX is an Erc-20 token backed by physical gold that has been fully audited and is stored in a vault in Singapore, known as the safe house (Schär, 2020). The value of each token is fully dependent

on the market value of gold. DGX is based on the Proof-of-Provenance algorithm where each gold bar is secured and its ownership/custodianship status is tracked accurately on the Ethereum blockchain. DGX is scheduled to be audited each quarter (every 3 months), making it more expensive.

2.5.2 Maker DAO (DAI)

Maker-DAO is an ERC-20 project that has a DAI coin. Unlike other stablecoins, Dai does not rely on a centralized entity or third party since it lives completely on the blockchain. DAI is a decentralized, cryptocurrency-backed coin (Lacity, 2020). DAI achieves price stability through an autonomous system of smart contracts called Collateralized Debt Position (CDP) that responds to varying market dynamics. To create new coins, Ether (ETH) must be used as collaterals and sent to the CDP. The CDP will lock the staked ETH and new DAI's will be minted. Maker DAO plans to allow for the use of other ERC-20 tokens in the future.

2.5.3 Basis

The basis is a stable coin that pegs its value through algorithmic adjustments of the coin's supply. Price stability is achieved through the monitoring of various external exchange rates that are verified by an oracle system (Kaal, 2020). If Basis is trading above 1, new stable coins are created and distributed. If, however, Basis coin is trading for less than1, Base Bonds which is another separate currency is created and sold in an open auction to take coins out of circulation.

2.5.4 Perth Mint Gold Token (PMGT)

Perth Mint Gold Token (PMGT) is a gold-backed coin, built on a public blockchain, backed by government-guaranteed gold (Jalan et al, 2021). PMGT is backed by a GoldPass digital gold certificate issued by The Perth Mint and guaranteed by the Government of Western Australia. Each

PMGT equals 1 fine troy ounce of physical gold. The supply varies constantly, increasing when Gold Pass certificates are exchanged for PMGT, and decreasing each time PMGT is redeemed for gold certificates. Like gold-backed cryptocurrencies, PMGT aims to simplify access to gold markets for institutional and retail investors and attract market participants desirous of participating in Fintech and blockchain innovations, but skeptical of the excessive volatility of cryptocurrency markets (Jalan et al, 2020). Having a government coming into play or a central issuer of a digital gold certificate creates centralization against the blockchain vision of decentralization.

2.5.5 PAX Gold (PAXG)

PAX Gold is a token on the Ethereum Blockchain, and it is backed by one fine troy ounce (t oz) of a 400 oz London Good Delivery gold bar, that is stored in Brink's gold vaults (jalan et al, 2021). It does not have any government guarantee unlike the PMGT, and its underlying physical gold is stored by Paxos Trust Company, regulated by the New York State Department of Financial Services. This also creates some elements of centralization within the PAX ecosystem.

2.5.6 Cardano (ADA)

Cardano is an "Ouroboros proof-of-stake" cryptocurrency that was created with a research-based approach by engineers, mathematicians, and cryptography experts. According to (Gaži et al, 2019), Cardano cryptocurrency is gaining ground due to the rigorous design process and seems to stand out among its proof-of-stake peers as well as other large cryptocurrencies. As of January 2021, Cardano has a market capitalization of $9.8 billion, and one ADA trades for $0.31. A report from coinCheckup (2021) indicates that Cardano cryptocurrency in March had a total supply of 31,463,134,114 coins and a 30 days volatility of 23.50%. Cardano is an algorithmic coin designed to achieve price stability and balance the circulating supply of the asset by using an algorithm

underneath those issues more coins when the price increases, and buys them off the market when the price falls.

2.5.7 Petro Cryptocurrency

Petro or petromoneda is a cryptocurrency issued by the government of Venezuela and was launched in February 2018. Its value is backed by the country's oil and mineral reserves, and was intended to supplement Venezuela's currency, as a means of circumventing U.S. sanctions and access to international financing (Chohan, 2018). It is backed by a barrel of oil from the Venezuelan crude oil basket and backed by flows of future mineable emissions. Having its value backed by physical certified asset reserves (Oil), it's very probable, therefore, that its price would be more stable. However, the underlying extractive reserves, whose price fluctuates on world commodity markets become a challenge. Oil and gas reserves also are hard to quantify not just in Venezuela, but in all other countries that export oil (Solarin et al, 2020).

2.6 Research Gap

From the literature, the researcher has noted that there is a gap in the existing models explored in the above section. The discussion below seeks to elaborate on these gaps;

The current online centralized payment services, such as Paypal, Apple Pay, Google Pay, Skrill, Amazon Pay, and Klarna, have a central company that acts as a thirdparty and preserves all inward and outward money transactions between e-commerce parties or those types of organizations that support online transactions. Although their development processes are simple, they are less secure, centralized, and subject to third-party control (central entity). The centralized payment gateways also charge high transaction fees.

The first wave of cryptocurrencies, such as Bitcoin (BTC) and Ethereum (ETH), ensured transactions directly from merchant to client or peer to peer, as well as validation through mining

via miners. Smart contracts, decentralized applications (DAPP), transparency, traceability, nonrepudiation, the possibility of cross-validation, and security (cryptographic nature) have all had a significant impact on their adoption. However, they have so far demonstrated high price volatility, scalability limitations, and complicated user interfaces.

The value of the Digix Gold Token (DGX), Perth Mint Gold Token (PMGT), and PAX Gold (PAXG) is backed by the actual value of gold. Even though their values are relatively stable due to the underlying gold value. The coin's volatility will be heavily influenced by the peg's value (If the Gold value fluctuates it swings the crypto value). Above all, the audit process for the system is expensive and time-consuming; thirdparties such as the vendors, custodians, and the project itself are needed to ensure the fullfunctioning of the system that underscores the capabilities of a decentralized blockchain.

Maker DAO is a decentralized autonomous organization. Adheres to a decentralized structure that is trustless, transparent, and secure. The liquidation process or conversion from one crypto to another happens quickly because it happens on the blockchain. However, because the underlying asset is a cryptocurrency, it is far more volatile than other assets such as gold. There could also be an instant liquidation since the underlying cryptocurrency can be instantaneously liquidated if its value falls below a certain threshold. Above all, multiple complex elements can obfuscate the minting process. In Petro cryptocurrency, the underlying extractive reserves, whose price fluctuates on local and world commodity markets. Oil and gas reserves also are hard to quantify.

On the other hand, Basis is designed to ensure that every adjustment is made on-chain and all data related to the stable coin is stored in a trustless, transparent, and secure ledger, it also removes the need for collateral to create a new coin; however, the rule-based system is integrated with complex logic that is hard to explain.

Table 1

Research Gap

	Model	Stabilization Approach	Weakness
1	Maker-DAO	Cryptocurrency-backed	1. Since the underlying asset is itself a cryptocurrency, it is inherently much more volatile than other assets such as Gold and Oil. 2. There could be an instant liquidation 3. Multiple complex elements within the system can obfuscate the minting process.
2	Perth Mint Gold Token (PMGT)	Backed By Physical Gold	1. The volatility depends on the value of the peg (gold) 2. It needs third parties such as the vendors and custodians 3. Centralization and a single point of failure are created by having a central custodian or vendor, 4. The audit process for the system is expensive and time-consuming
3	PAX Gold (PAXG)		
5	Digix Gold Tokens		
6	Cardano (ADA)	Algorithmic Adjustments	1. The Price volatility depends on the algorithm efficiency 2. The rule-based system is integrated with a complex logic that is hard to explain. 3. The audit process depends on the algorithm
7	Basis		

8	Petro Cryptocurrency	Oil and mineral reserves	1. The Price stability depends on the value of the Oil reserve. 2. Oil and gas reserves also are hard to quantify
9	Bitcoin (BTC)	None	1. High price volatility as shown in the historical charts 2. Limits to scalability 3. Complicated user interfaces
10	ETH (Ethereum)	None	

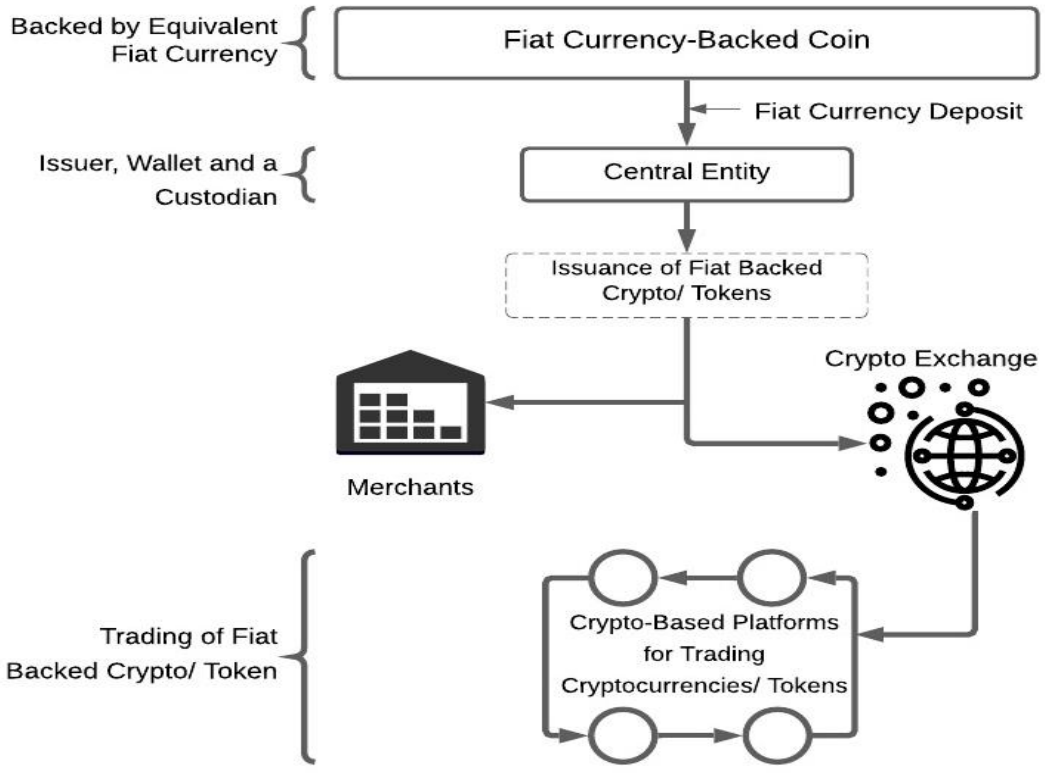
Although the existing stable coins examined seek to reduce price volatility, not much on ensuring 100% stability. The stabilization mechanisms placed by the government through the central bankensure that the shilling peg value can't be affected by the present cryptocurrency price volatility drivers. The peg reduces issues including market speculation, cryptocurrency market/technology maturity, and the lack of regulatory regulation and policies that trigger volatility. The envisioned model structure is easy to understand and has straightforward implementation procedures. The platform is aiming at creating a mutual integration of crypto-exchanges and traditional exchanges platform and provides transparency and accountability.

2.7 Conceptual Framework of the Study

The diagram below shows the conceptual framework.

Figure 6

Conceptual Framework



From the above diagram, the projected model will be creating a cryptocurrency that would achieve stability by pegging its value to less volatile KSh. (fiat currency) reserves. The cryptocurrency will be associated with the value of a Kenya shilling and holds its value fixed at a 1:1 ratio. This would offer complete stability compared to the volatility of other cryptocurrencies. The Kenya shilling price fluctuations are minimal. The fundamental point of the projected model is to create a cryptocurrency that would hold its pegged value. It would also ensure that despite the twists and turns of volatility that the cryptocurrency market faces otherwise. The underlying shilling peg value can't be affected by the present cryptocurrency price volatility drivers discussed insection 2.3.1. The peg mitigates issues such as market speculation, cryptocurrency market/technology maturity, and the absence of regulatory oversight and policies that cause volatility. The developed model would create a cryptocurrency that represents real money, which makes its price stable while enjoying the desired blockchain features. Accordingly, there is a central entity that manages the acceptance of new fiat currency and the issuance of a corresponding number of currencies. The central entity is the custodian of the fiat reserves that backs all the tokens. A third-party (smart contract) verifies and validates the fiat reserve to ensure it fully corresponds to the crypto supply. Whenever a holder wants to redeem cash with his tokens, the model will transfer the cash to the holder's bank account or the digital Fiat account for example M-Pesa and the equivalent coins will be destroyed or taken out of circulation.

2.7.1 The Model Synopsis

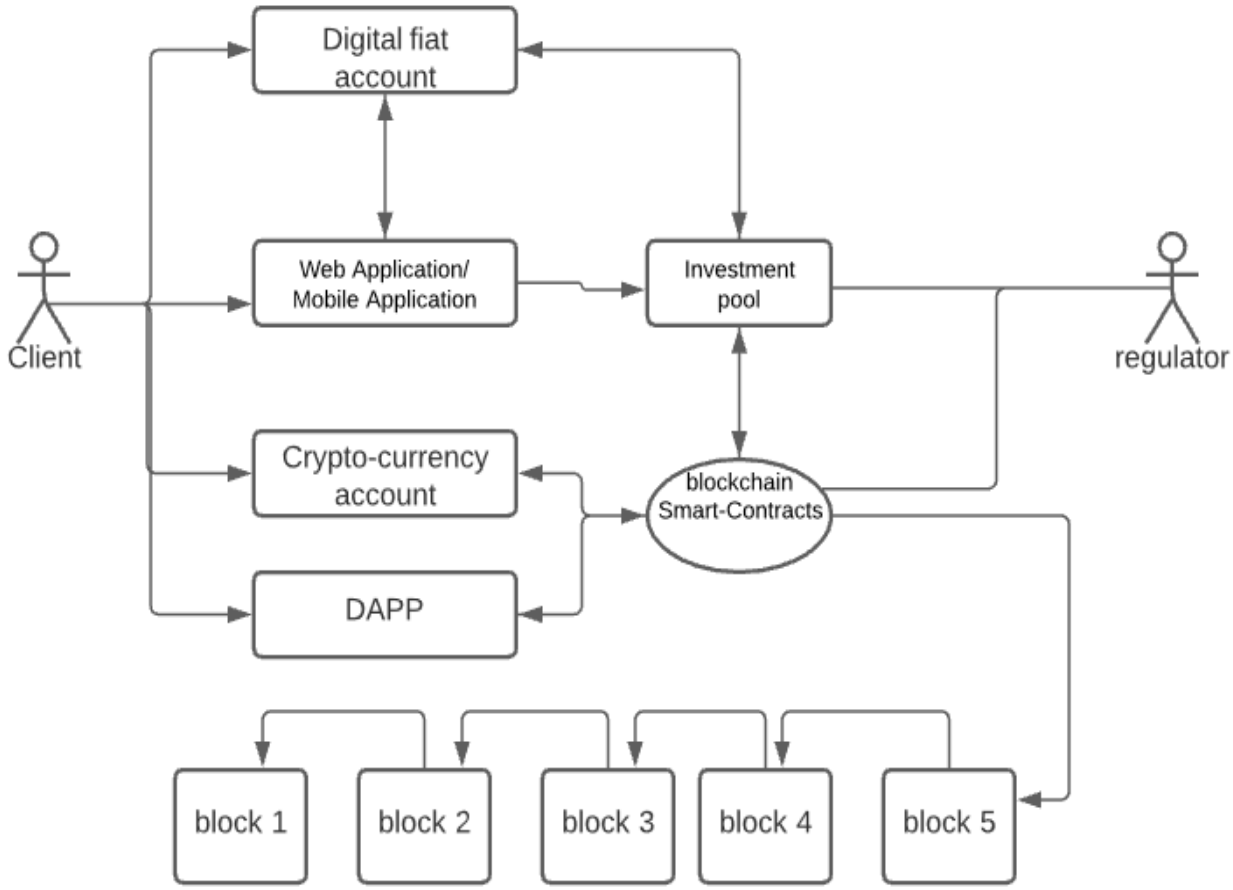
This idea proposes a stable-coin platform based on a shilling pegged approach where an individual who needs crypto-coins can interact with the stable coin provider. The platform is aiming at creatinga non-volatile cryptocurrency with a mutual integration of crypto-exchanges and traditional exchanges platform that provides transparency and accountability to the auditors. There

will be four types of participants in the proposed platform: investor (client), investment pool (smart contract), business, and auditor. An investor raises a request for a cryptoasset by submitting/ depositing an equivalent digital fiat currency to the platform. The smart contract (investment pool) invokes the crypto-pool to release crypto-tokens equivalent to the received digital fiat currency to the investor's crypto-account. The submitted crypto-tokens have to be captured in the blockchain architecture for suitability purposes.

2.7.2 Model Architecture

Figure 7

Proposed Model Architecture



2.7.2.1 Key to The Conceptual Framework

Client- Is a player in the stable currency ecosystem who is expected to be buying and paying for goods and services in the blockchain (stable coin infrastructure)

Digital fiat account- All clients are expected to own a digital fiat currency account. This research will be using Pesapal, PayPal, and M-pesa.

Crypto-Currency account- A platform user is expected to own a crypto-currency account or a crypto wallet to store both ethers and stable coins.

Web / Mobile application- The clients would access their accounts via the application API or direct through pre-provided methods by the service providers

DAPP- the clients would access blockchain-based service through the distributed applications (DAPP). The crypto-currencies would be used here as a medium of exchange or transaction fee.

Investment pool- the invested digital Fiat currency is stored in this pool. In the proposed research, the digital Fiat currency converted to crypto-currency is stored/ reserved here.

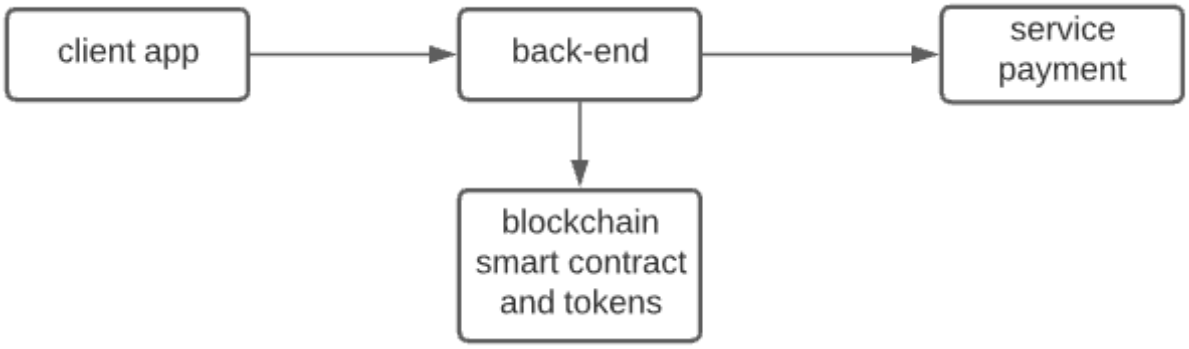
Smart contract- smart contracts are self-executing codes that create cryptocurrencies and print the transaction records (blocks) to the blockchain.

Blockchain- the distributed ledger that records the created coins is distributed and keeps track of the dissolved accounts.

2.7.3 Model Operation

Figure 8

Model Operation



i. **Fiat currency deposit-** 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 payment by the user, the backend receives the payment notification and sends it back to the smart contract for execution. If payment was successful the user receives equivalent tagged Crypto-Tokens.

ii. **Account dissolution -** 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 smartcontract.

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 deposits, account creation, account dissolution and withdrawals, token transfer, and exchanges.

iv. **Payment service -** Responsible for a token to shilling exchange by notifying the backend of any payment made.

2.7.4 Design Consideration

The principal design consideration for the proposed platform in this study would ensure decentralization, audibility, and openness, a greater degree of trust-minimization than an off-chain design. It would also consider asset flexibility where collateral can span all forms of digital fiat currencies.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.0 Introduction

Research methodology tells about how a researcher systematically designs research work to ensure reliable and valid results. Sing (2019), stated that research methodology comprises techniques or procedures that classify, scrutinize, process, and select information about specific issues or topics. This enables readers and researchers to analyze the overall validity and reliability of the research critically. Research Method deals with research tools and techniques to carry out research work. As Allen (2017) puts it, “research methods are procedures and schemes used in research and principally planned scientific”. Selecting a relevant research methodology and research method is very important to confine the study's robustness. This chapter will present the methodologies that were used in the collection of secondary data for review, model design, development, implementation, and evaluation.

3.1 Research Philosophy

Philosophy is derived from the word “Philein” which is the Greek word for “search for” and “Sophia” which means wisdom (Ndubisi, 2015). Wisdom is the capacity for sound evaluation and integration of facts. Knowledge is a comprehension of facts or personal acquaintance or familiarity with facts or ranges of information. Research philosophy is a belief about the way one pursues data collection, analysis and data use about a phenomenon. It is the basic belief system guiding the research covering the choice of method and includes three major aspects; ontology, epistemology, and axiology (Ramiz, 2016). Epistemology concerns what constitutes acceptable knowledge in a field of study, or what is known to be true. Ontology is concerned with social beings and focuses on the nature of reality. Ontology has two aspects – objectivism and subjectivism. Axiology is a

branch of philosophy that studies judgments about values and value systems (Mendie, & Eyo, 2016).

From the philosophical worldview, this research fell in the category of ontology Philosophy since the research is concerned with what actual existence of cryptocurrencies and volatility weaknesses that affect the adoption of blockchain and cryptocurrencies. The oncological questions that this research seeks to answer include;

i) Is there an existence of volatility weaknesses that hinder the absorption of cryptocurrencies?
ii) What causes cryptocurrency volatility?
iii) Are there measures that can reduce volatility in cryptocurrency?

Ontology philosophy guided and enabled this research to investigate through various methodologies, the existence of both problems and solutions towards achieving the objectives of this study elucidated earlier.

3.2 Research Design

Research design is a plan that guides the researcher in the process of collecting, analyzing, and interpreting observations. It is the researcher's blueprint for the methods and instruments used to gather information and evaluate it, to respond to the research questions (Eriksson & Kovalainen, 2015). Research design is also defined as a plan for selecting the sources, type of information, and the overall strategy that is used to integrate the different components of a study to effectively address the research problem (Ridzuan et al, 2018). It is a framework for specifying the process to achieve any research objective(s).

The overall methodology for this study was aproof of concept (POC) that aimed to demonstrate that the overall project idea is feasible. To achieve each specific objective of the study, different

methods were used. The integrative literature review (ILR) method was used to elicit weaknesses of the present cryptocurrencies thus addressing the first objective of this study. The integrative literature review method was appropriate because it compared information from diverse sources while addressingthe first objective to justifythe need for a new cryptocurrency model (before making a solid conclusion).

This research also adopted focus group discussions (FGDs) to obtain in-depth information from blockchain and cryptocurrency experts. The focus group discussion was first used to review and critically evaluate the cryptocurrency weaknesses derived from the integrative review process. Secondly, it was also used to investigate the proposed model requirements to facilitate the design. This helped in gathering deeper information about the model's functional requirement and its components and thus achieving objective two. To describe the model users and their potential tasks for the POC, the focus group discussions adopted a scenario-based design to evoke reflection in the model design.

The rapid prototyping approach was used in the model design implementation process. This was used to demonstrate various aspects of the model functionality and to realize the third objective of this study. Finally, the developed model was evaluated using functional testing. This was performed using the functional specification provided during the model design and verifies the model against the functional requirements. To evaluate the model quality, a metrics based on ISO 9126 quality framework was used. The model was subjected to pilot testing and the user feedback collected to ascertain the model quality.

3.3 Proof of Concept

Proof of concept (POC) is a realization of a certain method or idea to demonstrate its feasibility or a demonstration in principle to verify that some concept or theory has practical potential

(Cedarbaum, 2018). As shown in (Reed, 2017), the proof of concept (POC) or proof of principle (PoP) methodology is widely used in the fields of product design to describe objects, devices, or technologies that demonstrate the feasibility of how a thing may look or function.

This research illuminated through a case that "it is possible to improve the present cryptocurrencies and increase the adoption and usefulness of blockchain technology" through a PoC artifact. In this context, this research used a proof-of-concept approach to demonstrate and verify the practical potential of stable cryptocurrencies in the field of business and information technology via online trading. The primary purpose was to verify the viability of stable coins that are based on fiat currency.

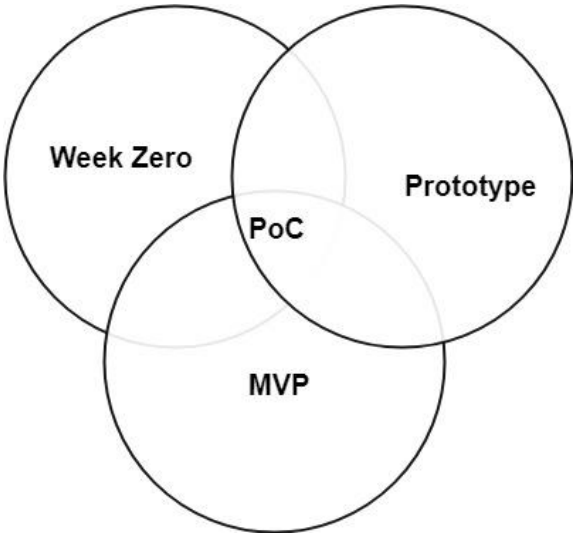
This methodology aims to avoid spending a lot of money (resources) on something that is not feasible market-wise or technology-wise. As stated in Augusto (2017) and Gordon (2017) this method gave chance to get tangible proof that the overall research idea was worthwhile.

3.3.1 The Proof-of-Concept Procedure Phases

As pointed out in the research design section, this research used a proof-of-concept methodology to address how the model supported the envisioned goals, objectives, and other upcoming business requirements. This involved clearly defining criteria for success, documentation for how the proof of concept was carried out, and an evaluation component. This study used a focus group discussion and scenarios to define model functional requirements and evaluation criteria via potential user stories. At the end of the model implementation, the model prototype performance was evaluated using function testing evaluation techniques.

Figure 9

The Proof-of-Concept Procedure Phases



The POC methodology was carried out in three phases; week zero, prototype, and minimum viable product (MVP). During Week Zero, this research carried out a general literature review to prove the need for stabilized cryptocurrency based on fiat currency for online-based businesses. This also demonstrated how the stable cryptocurrency would improve cryptocurrency adoption and ensure stable cryptocurrency as an alternative to the present cash. In general, this stage (week Zero) gave a clear theoretical postulate ready to be tested.

The prototype phase developed a model prototype to affirm and demonstrate the feasibility and practical potential of the research idea. This intends to inform the researcher and other decision-makers to determine how best to develop the product when it moves into full production for a final/ market-ready item as pointed in (Kesebi, 2019).

Similarly, a Minimum Viable Product (MVP) came after successful prototyping of the proof of concept (Tripathi et al, 2018). In this stage, a product with a minimum set of features that are viable

enough to test the research's fundamental assumptions was created. The MVP was used to prove the model's postulate with minimal resources.

To further expound on the above PoC phases, the proof of concept will be further broken and carried out in five steps namely planning, designing, implementation, operation, and improvement (PDIOI) as shown in the following section.

3.3.2 PDIOI Approachfor the Proof of Concept

The prototype design, implementation, and evaluation were carried out in five phases. This includes Planning, Design, Implementation, Operation, and Improvement. PDIOI is Huawei's methodology for Implementing Enterprise Engineering Project (IEEP) (Huawei, 2020). This methodology was ultimate as aided in improving agility, Fast-moving processes, and lowering and addressing complexities during the PoC artifact implementation.

i) Planning

The planning phase looked at the model’s background, requirements, and objectives analysis as well as determining the technological road map. It reviewed the model from a macro view and set out a framework for the entire research. It also determined the general orientation which directly influenced the model's achievements. Lastly, it was the guiding principle for the model design. In general, this phase was important grasping the general background of the research, ensuring a sound exterior environment for smooth development.

ii) Design

In this phase, the model design based on the model requirements and guidelines specified in the planning phase was implemented through technological methods. The model design phase followed the recommendation and scenarios created during the focus group discussions. Through

the focus group's SBD in this phase, the device selection, technological roadmap, model functionalities, and performance specifications were determined.

iii) Implementation

The model was built and the additional components were incorporated according to the design specifications, Supporting infrastructure, and governance.

iv) Operation

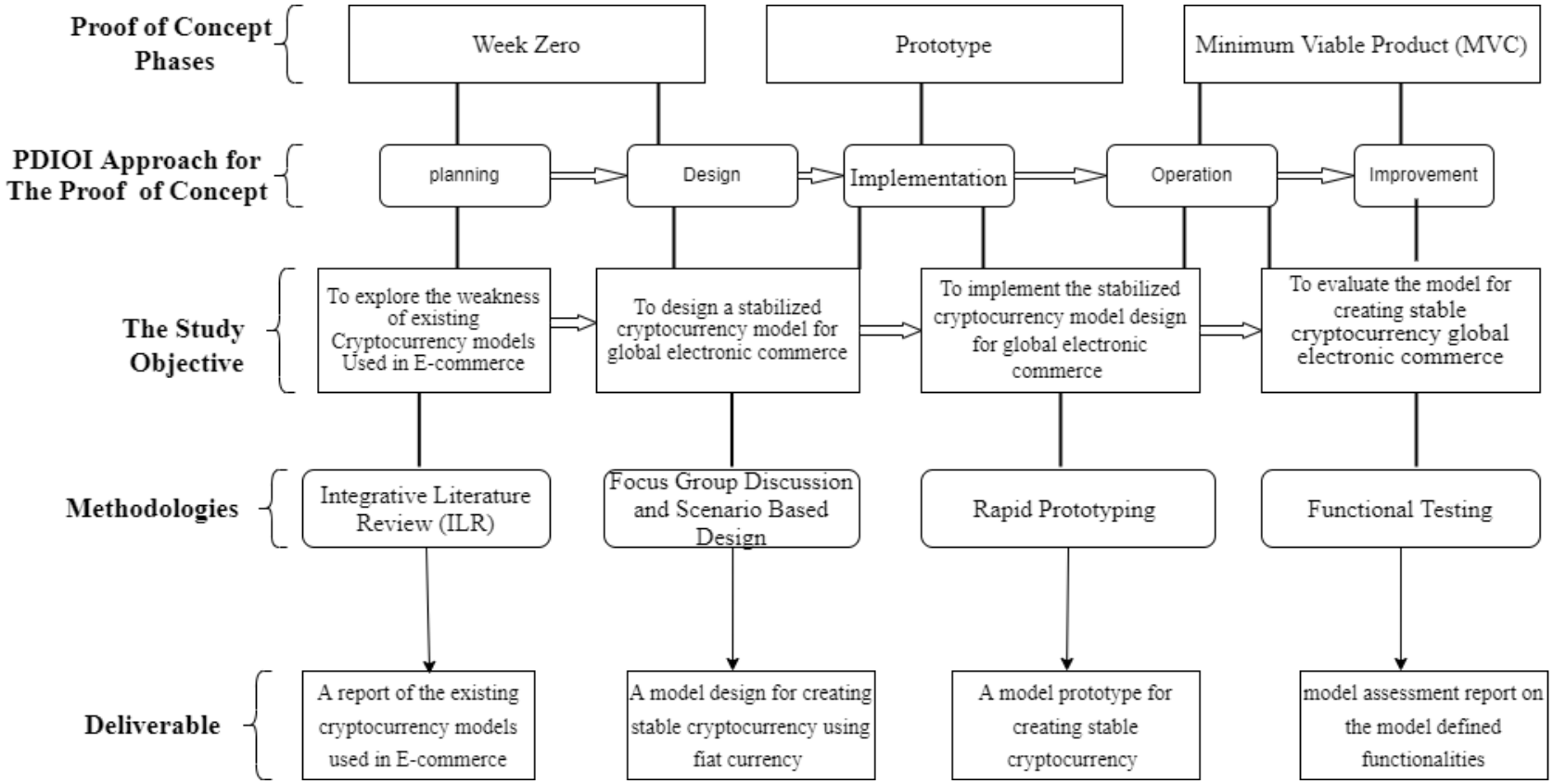
The model's working and vital signs were proactively monitored for improvement. This phase provided a framework and operational tools to respond to problems.

v) Improve

The model performances, security, usability, and user experience were improved.

Figure 10

The Proof-of-Concept Process for the Model for Creating Stabile Cryptocurrency Using Fiat Currency for E-Commerce



3.4 An Integrative Literature Review Methodology

An integrative review is a broad type of research review method that allowsthe inclusion of experimental and non-experimental literature to provide a more comprehensive understanding of a particular phenomenon of concern (Scupola et al. 2021). The purpose of this methodology was to identify and review diversesecondary data sources relevant to the first objective of this study. The first objective aimed to determine the weaknesses in the existing Cryptocurrency models used in E-commerce. The importance of this was to scrutinize and identify the weaknesses in the present collateralized and non-collateralized coins. Subsequently, these would guide the design and implementation of a model that would resolve price volatility weaknesses in cryptocurrencies that have inhibited rapid adoption in online-based trading for the provision of alternative cash. The integrative literature review inclusion of both secondary research studies, along with other documents (including opinions, discussion papers, policy documents, and reports from focus groups) provided a diverse source of information.

To develop an evidence-based approach for the ILR, the Critical Appraisal Tool was used. Qasim & Kharbat (2019) stated that this method allows researchers to authenticate the research evidence and check the reliability of the study. The CASP tool enables the researcher to make a critical assessment and validate the secondary data and reduce the chances of unauthentic or unreliable data in the study. This method was preferred because it improves the existing data's reliability and facilitates the imminent appraisal practice. The current study's CASP approach was used to strictly analyze and study the validity of the weaknesses of the present cryptocurrencies used in e-commerce. This encouraged the researcher to check whether there was any need for a new form of cryptocurrency based on the shreds of evidence found in the literature.

3.4.1 Integrative Literature Review (ILR) Methodology Inclusion and Exclusion Criteria

Inclusion criteria deal with the study's characteristics and features, which must be included (Min, 2019). In contrast, exclusion criteria comprise the set of characteristics that need to filter out and exclude from the study. Inclusion and exclusion are the eligibility criteria, which can help improve the study's accuracy and produce sound and evocative results. The inclusion and exclusion criteria set for the current study are given in the below table.

Table 2

Material Inclusion and Exclusion Criteria

INCLUSION	EXCLUSION
i) The articles published in 2016-to 2021	i) Irrelevant, unauthentic, or zero cited
ii) Articles having good impact factor	ii) Materials older than 2015
iii) Articles from popular computer science and information technology-based databases	iii) Irrelevant factors must not be included in the study
iv) Having keywords: Stable Cryptocurrency, Fiat Currency, cryptocurrency weaknesses, cryptocurrency in E-commerce	iv) UK Essay, blogs, and Wikipedia
v) The relevant aim, objectives, or hypothesized research articles, reports, thesis, and research papers (note: the literature type is ILR)	v) Other than the English language
	vi) Incomplete research materials

vi) Supportive Qualitative and Quantitative materials

vii) English Language

viii) Complete abstract and practical implications with study limitations

ix) Articles published after 2015

3.4.2 Integrative Literature Review Framework

To enhance rigor during the review process, this review was guided by Whittemore and Knafl's framework for literature review. This framework defines the process of conducting a research review as incorporating a problem formulation stage, a literature search stage, a data evaluation stage, a data analysis stage, and a presentation stage (Whittemore & Knafl 2005).

ILR Step 1: Integrative Review Problem Identification

Theoretical and empirical work in the past related to the rapid growth of the internet and digitization of enterprises shows that the monetary sector is significantly affected due to the striking growth of e-commerce and e-payments. However, the concept of globalization of financial services and cross-border banking performance shows that current payment systems still have two major weaknesses: lack of universal access to financial services for a large portion of the world's population and inefficient cross-border retail payments. The introduction of digital ledger technology and cryptocurrency was intended to address these problems but they experience short-term extreme price volatility. Therefore, the purpose of this integrative review was to analyze the concept of cryptocurrency volatility and other weaknesses.

ILR Step 2: Integrative Review Literature Search

The literature search was comprehensive but with a specific focus on blockchain and cryptocurrency volatility facilitated the literature search stage. The search used "cryptocurrency volatility" as the keyword on the selected scientific search database. The selection criterion for the research databases was based on the total number of articles, conferences, and bibliographic entries. ACM Digital Library academic search database for computer science with the highest articles and bibliographic entries was used.

To cover a broad set of publications, the database was searched with the following string in the title, abstract, and keywords: {(cryptocurrency volatility) AND (publication date (01/01/2015 TO 09/30/2021))}. To ensure comprehensiveness, this research identified three eligible primary strategies as suggested by (McCarthy et al 2018). These include database searching, ancestry searching, and hand searching. On searching the identified database between2015 in Sep 2021, we identified 903 articles as shown in appendix v, and 182 articles from other sources.

To identify and filter data sources, the study initially checked the importance of each article by analyzing the title, abstract, and keywords. If any sign of relevance appeared, the source was marked for further analysis. The study excluded sources that were duplicates, grey literature (i.e., editorials, work-in-progress), not applicable to the study, or not available in English as guided by the inclusion and exclusion criteria. This first relevancy assessment resulted in a sample of 620 potentially relevant articles. Afterward, a fine-grained relevance validation was made by accessing and reading the article abstracts, resulting in a final sample of 191 relevant sources. In this second relevance assessment, we excluded non-research articles and articles that did not relate to the volatility of cryptocurrency as shown in the PRISMA Tool Flow Chart in figure 16. EndNote citation management software was used to keep track of the articles reviewed.

ILR Step 3: Integrative Review Data Evaluation

The final sample for this integrative review included several reports. Reports from focus groups, case studies, instrument development designs, and cross-sectional. Due to this diverse representation of primary sources, this research used PRISMA Checklist (critical appraisal tool) to assess the informational value and quality of potential sources before they are included in the final report. No report was excluded based on this data evaluation rating system; however, the score was included as a variable in the data analysis stage. In general, reports of low rigor and relevance contributed less to the analytic process.

ILR Step 4: Integrative Review Data Analysis

The study carefully reviewed and analyzed the 191 sources to identify cryptocurrency weaknesses and the potential causes. For each weakness, a name, description, source, and weight to show the frequency was recorded. A list of main features was created to aggregate the identified cryptocurrency weakness. The main feature is an aggregation of similar weaknesses consisting of the main feature name and the main feature description. If weakness fits into an existing main feature, the researcher assigned it accordingly; otherwise, a new main feature was created. For example, we aggregated the weaknesses “computer-generated” and “no physical form” to the main feature “virtual”. The researcher also aggregated the weakness “potential for large losses” and “Valuation Fluctuates” to the main feature volatility.

Since different authors use different terms for the same weakness, we considered semantic ambiguities during the data analysis. To improve the readability of this research work we usedthe cryptocurrency weakness for the main feature in the remainder of this document since the main features represent the aggregation of similar weaknesses. To ensure that the study identified a reliable set of main features, the research aimed to reach theoretical saturation concerning the

emerging weaknesses. Since no new main feature emerged in the last 27 data sources identified in the literature review, the team was confident it have reached theoretical saturation (The researcher reached a point in the analysis of data that sampling more data sources could not lead to more information related to cryptocurrency weaknesses).

To consolidate and critically evaluate the derived cryptocurrency weakness and their respective description, a focus group was formulated to review and provide feedback. The focus group discussion participants consisted of blockchain experts who had experience in dealing with blockchain. The focus group discussion formulation criterion is shown in section 3.3. The final weaknesses and their description were revisedaccording to the focus group outcome. For example, composite weaknesses were split into primary weaknesses.

ILR Step 5: Integrative Review Presentation

After the focus group review of the identified cryptocurrency weaknesses, 18 cryptocurrency weaknesses were revealed. To enhance visualization and interpretation, the 18 weaknesses are briefly described and presented in the matrix Table 3.

3.5 Focus Group Discussion

A focus group discussion (FGD) involves gathering people from similar backgrounds or experiences together to discuss a specific topic of interest (Nyumba et al. 2018). It is a structured discussion used to obtain in-depth information from a group of people about a particular topic. In this study, this method aimed to obtain data from a purposely-selected group of individuals with blockchain and cryptocurrency experience. According to Van and Angehrn (2017), FGD has five characteristics that suited this methodology in this study. These include;

i) Multiple participants with common characteristic(s) that is (are) meaningful from the research perspective.

ii) Semi-structured; carefully planned and cautiously executed.

iii) Often a large spectrum of opinions, notions, and/or experiences; added focus on social interaction between participants.

iv) High level of focus on the given topic

v) When accurately and adequately moderated, all participants contribute equally to the discussion

Van and Angehrn (2017) also recognized natural groups and expert groups as two types of focus groups. Natural groups consist of multiple participants who belong to a pre-existing informal or formal group (e.g., family or kin, co-workers) before the study. While expert groups consist of several people who have particularly good and broad expert knowledge and experience of the research topic(s). They also added that such groups tend to be smaller than typical FGDs and are used to solicit large amounts of highly specific information, although participant statements may vary.

With respect to Van and Angehrn's (2017) classification of focus group discussions, this research used expert groups. The focus group discussion participants consisted of blockchain and cryptocurrency experts as shown by the participant inclusion criteria. The expert focus group discussions (EFGDs) were used to first review and critically evaluate the derived cryptocurrency weakness recorded during the integrative literature review. Secondly, it was used to investigate the model requirements for design purposes. This helped in gathering deeper information about the model's functional requirement and its components. At the end of the focus group discussion, a description of model functional requirement, model inputs, outputs, and the expected behavior was realized.

3.5.1 The Focus Group Discussion Operational Planning

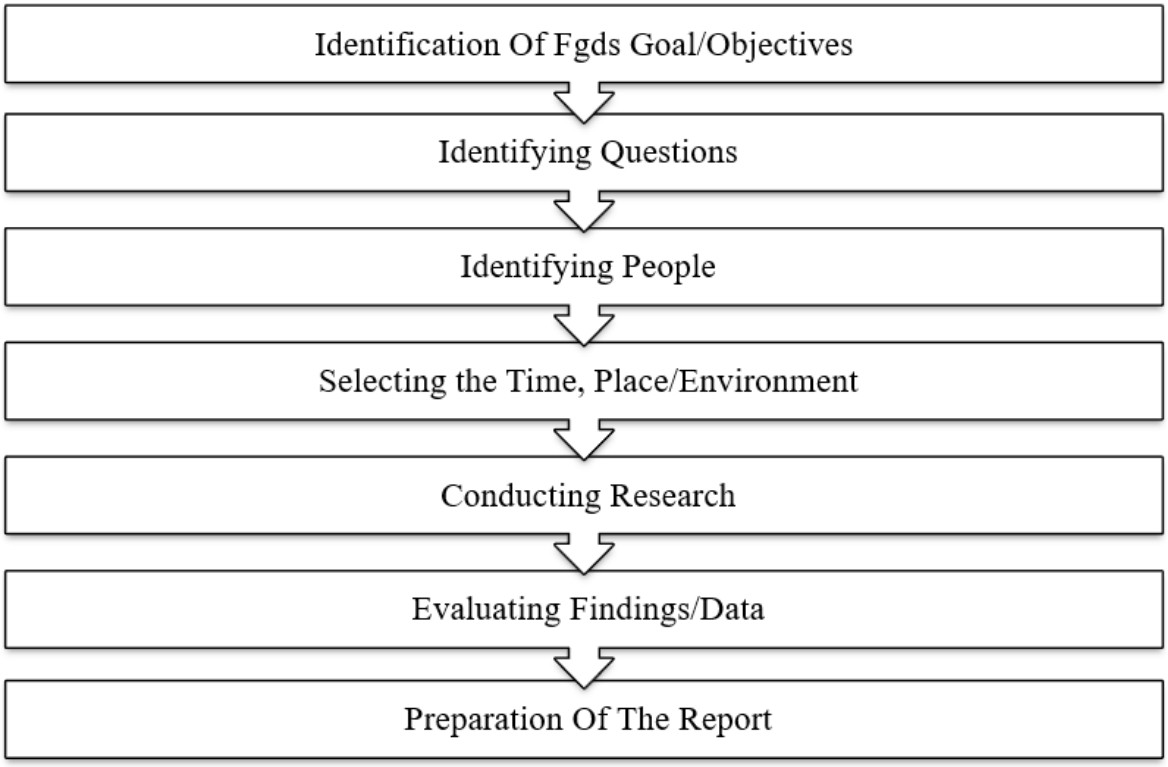
Before the FGDs, some operational planning for the exercise was undertaken. These include: preparing and developing informed consent forms and a comprehension list in line with research ethics best practices. The research team also obtained official approval from the ethical committee (From KUREC) and NACOSTI. Time and place planning for the interviews were also organized. The interview places selection considered venues that would allow for a relaxed, safe, and comfortable interaction. The recording tools and equipment were also arranged.

3.5.2 Glynn, Shanahan, and Duggan (2015) Framework for Conducting a Focus Group

To conduct the focus group discussions successfully, a framework recommended by Glynn, Shanahan, and Duggan (2015) was used. It involves the identification of FGDs goal/objectives, identifying questions, identifying people, selecting the time, place/environment, conducting research, evaluating findings/data, and preparation of the report. To enhance the readability of this research work, the researcher summarised these phases into major and sub-phases while acknowledging the source.

Figure 11

The Process of FGD



Step 1: The Focus Group Discussion Purpose

The purpose of the focus group discussion was to review the cryptocurrency weakness recorded during the integrative literature review. This ascertained that the recorded weaknesses were within the cryptocurrency domain and were atomic. It also identifiedthe model's requirements and its components for design. Through the FGDs, the categories of users' and stakeholders' different perspectives and requirement needs were elicited and prioritized.

Step 2: Focus Group Discussion Discussion Prompts/ Questions Identification

Before the focus group discussion, a list of questions and discussion prompts that would help gather information were created. The questions were formulated in three dimensions: (i) questions that would seek to review the derived cryptocurrencies' weaknesses from the integrative review

process, (ii) those that aided in the dependency and best platform identification, and (iii) those that would aid to gather information about the potential model users and their requirements. These are shown in the guidelines for conducting the focus group appendix iv.

Step 3: Selecting the Participants and Leader

The focus group discussion participants targeted blockchain experts who had experience in dealing with blockchain. The research identified four blockchain-based companies which the participants would be sampled from. A letter was written to seek formal permission to carry out the research in the identified institutions (a sample letter is shown in appendix vi) or a phone call. For the organization that had a policy about research activities, the research team read the policy and determined the appropriate process to gain access to the people. The research team also presented the obtained official approval of an ethical committee (From KUREC), ethically approved data collection tools and procedures, and the NACOSTI clearance.

Upon receiving approvals from the institutions to carry out the research, the research sampled between 4-7 members per group as guided by Krueger and Casey (2002). To ensure compliance with research ethics best practices, the researchers obtained informed consent from the potential focus group participant through the informed consent form presented in appendix I. The process of obtaining consent from the participants was also guided by the approved procedures presented in appendix ii. Before the focus group discussion, all the participants were asked to complete a comprehension checklist questions survey that explored the participant's familiarity with the focus group discussion objective, their expectation during the discussion, and their perception of the value of the entire research objective. The survey consisted of open-ended questions as shown in appendix iii. The information was used to help gauge the participants' familiarity with the discussion topics.

The research also selected one focus group leader who is outside of the organization to ensure participants aren't fearful of backlash or lead tobias and skewness. The research also ensured that the leader is familiar with the research topic since it followed the other participant's recruitment criteria. The leader or facilitator selection was also based on his/her ability to build rapport by creating a warm, supportive and comfortable environment to foster open and honest dialogue among the individuals. At the end of the selection process, each focus group discussion consisted of at least four members and the largest group had six members

Step 4: Selecting Time, Place/Environment

This research identified the time and place of the discussion based on the participants' convenience. It considered participants' comfort, access to the venue, and levels of distraction. A normal and familiar setting with sufficient space for different activities within the focus group discussion, such as note-taking, evaluation of comprehension, and internet access was considered. Before the focus group discussion, the research team ensured that there was enough seating that enabled participants with a clear view of each other and the facilitator/ the focus group leader. The researcher also communicated the agenda, location, and time to the focus group participants ten days earlier.

Step 5 Conducting Research

Each focus group discussion started with an introduction of the research team and the selected leader. The purpose of the focus group discussion, focus group discussion rules, how to ensure confidentiality, and the participant's role was also explained. Nyumba et al. (2018) recommended a minimum of three to four group meetings for simple research topics. To ensure that the focus group discussions yield maximum impact on the research and the theoretical saturation realized, this research carried out four different focus group discussions.

Before the discussion, the participants agreed on the way of documenting the FGD findings. A minute/ note-taker was enlisted to write down the most important points made by participants, along with any other ideas or analytical thoughts that come to mind during or right after the discussion. To ensure that no important point was left out, each focus group participant was given a notebook and a pen to record what they found important during the discussion to complement the note-taker.

In two of the carried focus groups, a group exercise to search for some content online and the projected model user role play was incorporated into the course of the discussion to formulate scenarios for design. The scenarios created during the focus group discussion are presented in section 4.2.4 below. The facilitator followed the approved guidelines shown in appendix ii and all the guiding questions were discussed. At the end of the discussion, the notetaker read out the recorded findings for the participants to ascertain and add if there was an important point left out. The final focus group findings were labeled with a unique focus group id and stored for further analysis in the next phase.

Step 6: Evaluating Findings /Data

This stage coalesced the focus group discussion into a manageable form for report development. This phase began immediately after focus group closure. The Comprehensive note-taking and summarization of the discussion with the participants during the focus group session facilitated more efficiency in this phase. For each focus group question, the findings were summarized into a functional requirement or design consideration. Data reduction was the key to this stage; the discussion was summarized into manageable concepts that will facilitate report development or model users and their possible functional requirements.

Step 7: Focus Group Discussion Report.

This phase summarized the key findings of the focus group discussion conducted with the blockchain and cryptocurrency experts. The focus group discussions revelation is presented in form of the model objectives and design principles that would inform the model design and implementation.

3.6 Scenario-Based Design for the Model Design

According to Hanington & Martin (2019), Scenario-based design is a family of techniques in which the use of a future system is concretely described at an early point in the development process. Narrative descriptions of envisioned usage episodes are employed in a variety of ways to guide the development of the system. As Rosson and Carroll (2009) put it "a scenario describes a specific target user trying to achieve a specific goal or perform a specific task in a specific context." In other words, scenario-based design is a relatively lightweight method for envisioning future use possibilities. Concisely: scenario=user + task + context.Scenarios evoke reflection in the content of design work, helping developers coordinate design action and reflection. These qualities, the concrete and work-oriented nature of scenarios make them effective for the envisioned model design activities.

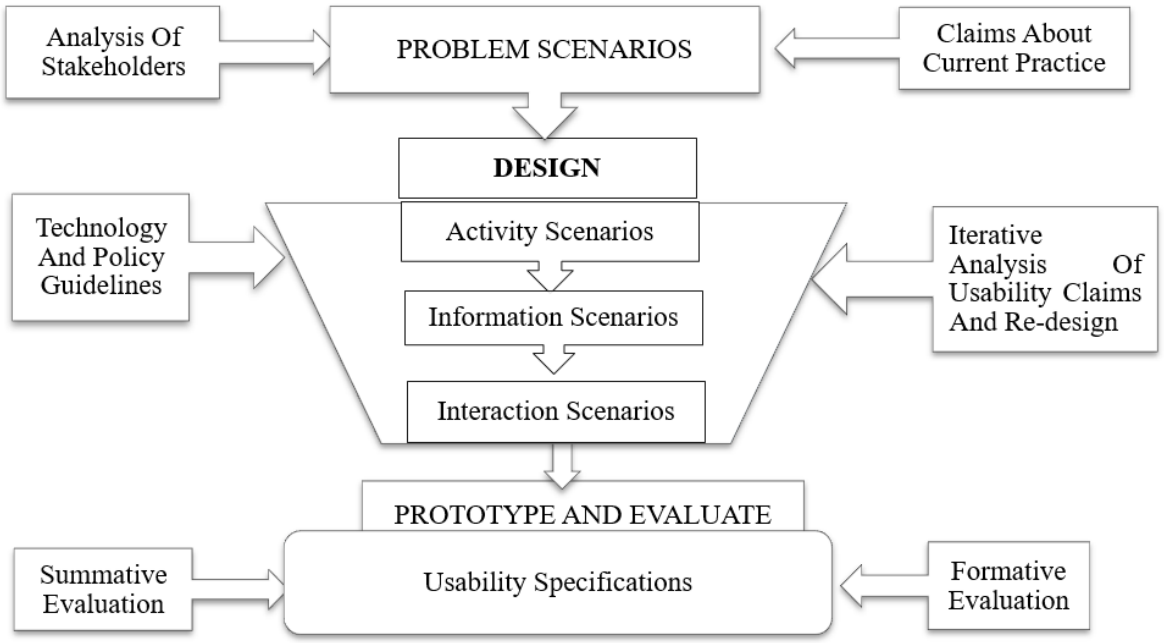
During the focus group discussions, the scenario-based design was employed to present a concrete and flexible design. Scenarios gave multiple views of interaction and diversity helping the researcher manage the model design. It helped to recognize, capture, and reuse generalizations in the model design.

To employ scenarios-based design in this study, a framework presented by Rosson and Carroll, (2009) in his book entitled Orchestrating human-centered design was used. This framework incorporates scenario-based analysis and design into all phases of system development, from

requirements analysis through usability evaluation and iterative development. The overall process in this study aimed at improving usability, where the scenarios supportedthe identification of model requirements and elaboration of the model's usefulness. The aim was to develop a rich understanding of model elements, platform specification, model functionalities, and how to implement them. It also helped to use this understanding as a basis for activity transformation while observing the model design philosophies. Figure 1 provides an overview of the scenario-based design framework used in this study.

Figure 12

An Overview of the Scenario-Based Design (SBD) Framework



In SBD, scenarios serve as a central representation throughout the model design and development. Firstly, a description of the model goals and concerns of current use, and then being successively transformed and refined through an iterative design and evaluation process. The problem scenarios were transformed and elaborated through several phases of iterative design as suggested by Rosson

and Carroll (2009). The definition of scenarios utilized focus group discussions where blockchain and cryptocurrency expert members describe the potential user, task, and context. The designed scenarios are presented in the next chapter.

3.7 Smart Contracts Design

The objective to design a model for creating a stable cryptocurrency using fiat currency for E-commerce involvedthe design ofa system of smart contracts. To write a secure and scalable smart contract back-end, this model was distributing the data and logic over multiple smart contracts. The design architecture for the developed model as a system of smart contracts, therefore, was based on the design principle of having different types of contracts to perform different classes of tasks. To classify the contracts, a "The Five Types Model" model is used (Monax, 2017), although all or some of the five models might be used in the proposed POC. This model divides contracts into Application logic contracts, Contract managing contracts, Controller contracts, Database contracts, and Utility contracts.

i) Database Contracts

These Contracts are used as data storage. The only logic they need is functions that allow other contracts to write to, update, and get data and some simple way of checking caller permissions (whatever those permissions maybe).

ii) Controller Contracts

One step up in the layer of abstraction is a contract for controlling database contracts. These contracts operate on storage contracts. In a flexible system, both controllers and databases can be replaced by other, similar contracts that share the same public API (although this is not always needed). Controllers can be advanced, and could, for example, do batch reads/writes, or read from

and write to multiple different databases instead of just one. They can also act on multiple database contracts.

iii) Contract Managing Contracts (CMCs)

These contracts are needed to control and manage the actions and existence of other contracts. Their main task is to keep track of all the contracts/components of the system, handle the communication between contracts and other components, and make modular design easier. Keeping this functionality separate from normal business logic should be considered good practice, and has several positive effects on the system (as we will see later).

iv) Application Logic Contracts (ALCs)

Any contract that is implementing application-specific code tasks through controllers is anapplication logic contract. Generally speaking, if the contract utilizes controllers and other contracts to perform application-specific tasks it's an ALC.

v) Utility Contracts

These types of contracts usually perform a specific task and can be called by other contracts without restrictions. It involves some small, generic functions that can be outsourced into highly specialized utility contracts. It could be a contract that hashes strings using some algorithm, provide random numbers, or other things. They normally don't need a lot of storage, and often have few or no dependencies.

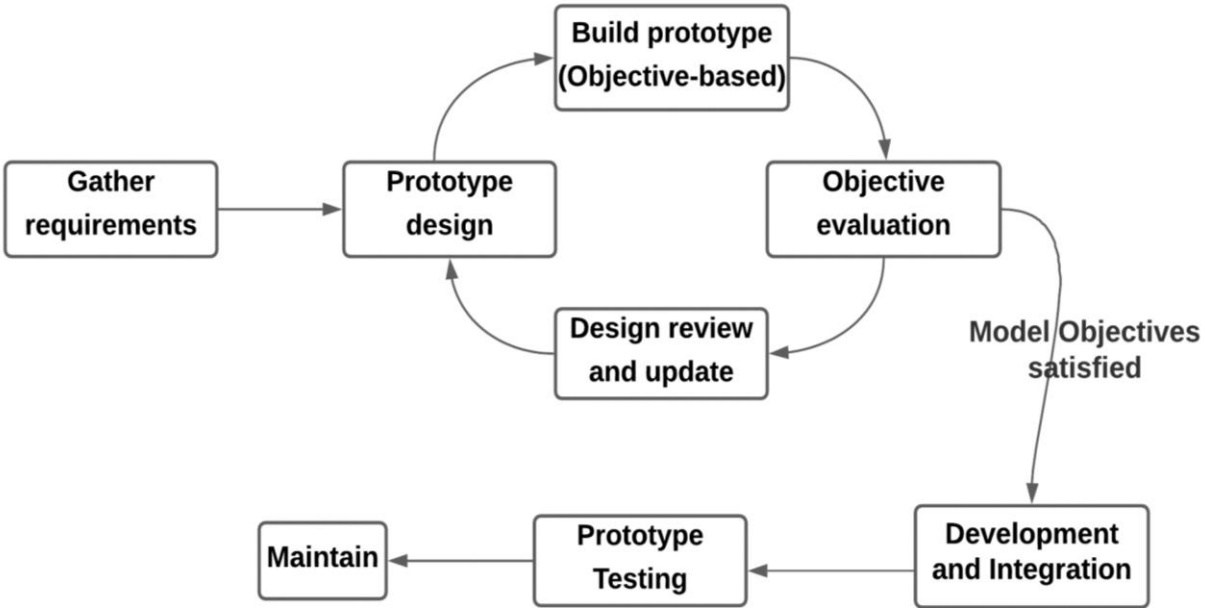
Based on the above-proposed monax model and the PoC functional requirement, the proposed model design proposed several contracts that worked together to realize the overall objectives and goals of the study.

3.8 Model Development

The study aimed at developing a model for creating a stable cryptocurrency that backs its value to that of the Kenya shilling. This allows it to utilize all the price stabilization mechanisms placed by the central bank to lower volatility. The rapid prototyping approach described in the figure below was used in the model implementation process. A prototype is a model of a product or a system in part or whole (Menold et al, 2017). Rapid prototyping (RP) is the act of creating a low-fidelity object to test a concept (Menold et al, 2017). The rapid prototyping approach depicted in the Figure below was used in the translation of the proposed model design into a functional prototype.

Figure 13

The Stable Cryptocurrency Model Prototype Implementation Processes for E-Commerce



a) **Gather Requirements**

Based on the information gathered from the first objective of this study, this research considered volatility weakness that was mentioned in all the reviewed literature. This phase of the RP entails the information from the literature review and the information gathered from the focused groups on the minimum functional requirements for the model and a report to overcome the weaknesses of the existing models. The requirement gathering is shown in section 4.2.4.

b) **The Model Prototype Design**

In the design phase of the prototype, designs based on the model requirements and guidelines specified were implemented through technological methods. This phase followed a modular design principle and hierarchical architecture.

This phase involved various model design processes such as;

i) Identification of the Most Suitable Consensus Mechanism.

A Proper consensus mechanism that is energy efficient, secure, and fast will be identified.

ii) Identify the Most Suitable Platform

Based on the consensus mechanism criteria, a good chain was selected that would support all the qualities identified in section 4.3.7

iii) Designing the Blockchain Nodes

This included the type of service either mobile-based or web-based. It also included how to treat an off-the-chain transaction.

iv) Designing the Application Programming Interface (APIs)

v) Design User Interface for both expert and amateur users.

vi) Bridge mechanism

vii) Underlying architectural design

viii) Digital fiat currency platform integration design

c) **Build Prototype**

During the RP implementation stage, the model was built and the additional components were incorporated according to the design specifications, Supporting infrastructure, and governance. Building the prototype included and not be limited to the following steps.

i) Definition of a series of Environment Setup steps

ii) Functional decomposition and implementation

iii) Integration of separately implemented modules /parts

iv) Smart contracts development (following the proposed modular monax model depicted in section 3.4)

v) Selection and implementation of user interface development tools

vi) Wallet design and integration

d) **Prototype Testing**

Prototype testing involved functional testing, smart contracts testing, integration outcomes, and all the functional and quality attributes that were defined during the requirements gathering and the prototype planning. This involved both off-the-chain and post-chain deployment testing. All the components of the prototype were considered fit for its task once a transaction process (initiation, validation, and storage) was complete and stored within the blockchain network.

3.9 Model Evaluation

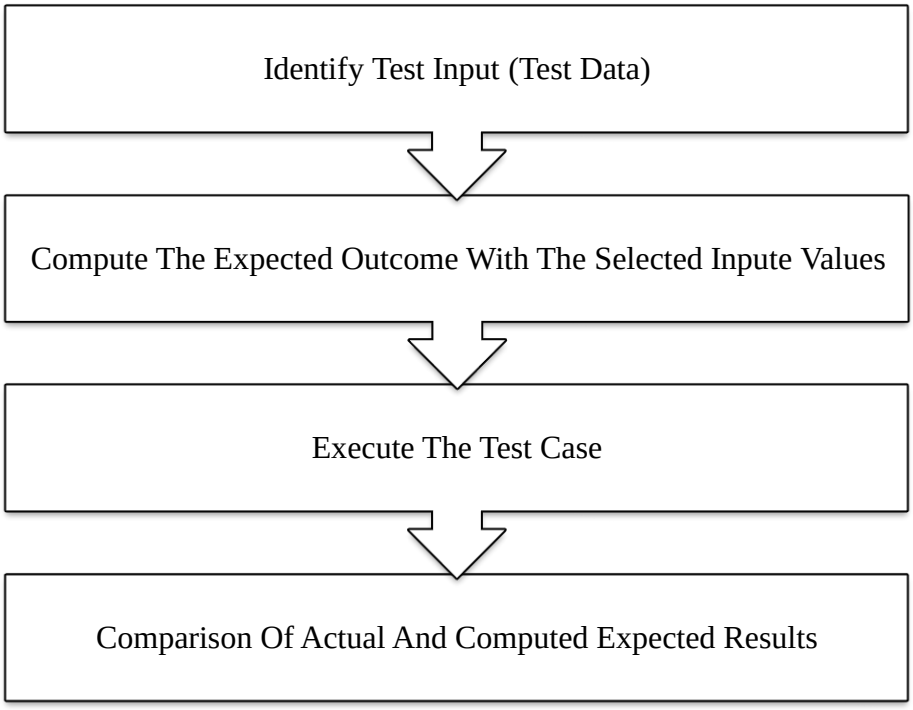
The developed model for creating a stable cryptocurrency using fiat currency for online trading was evaluated using functional testing. Functional testing/ evaluation was performed using the functional specification provided during the model design and verifies the model against the functional requirements (Chung et al, 2012). The functional evaluation deals with attaining the defined functional requirements. The purpose of Functional tests is to test model functionality, by providing appropriate input and verifying the output against the functional requirements.This testing checkedthe User Interface, APIs, Database, Client/Server communication, and other functionality of the model. The evaluation mainly concentrated on;

1. Mainline functions- testing the main functions of the developed model
2. The model basic Usability – involved the basic usability testing of the model. It checked whether a user (expert user in this case) can freely navigate through the screens without any difficulties.
3. Accessibility- Checked accessibility of the model functionalities
4. Error Conditions: Usage of testing techniques to check for error conditions and to check whether suitable error messages are displayed.

3.9.1 Description of Evaluation Criteria

Figure 14

Description of Model Evaluation Criteria



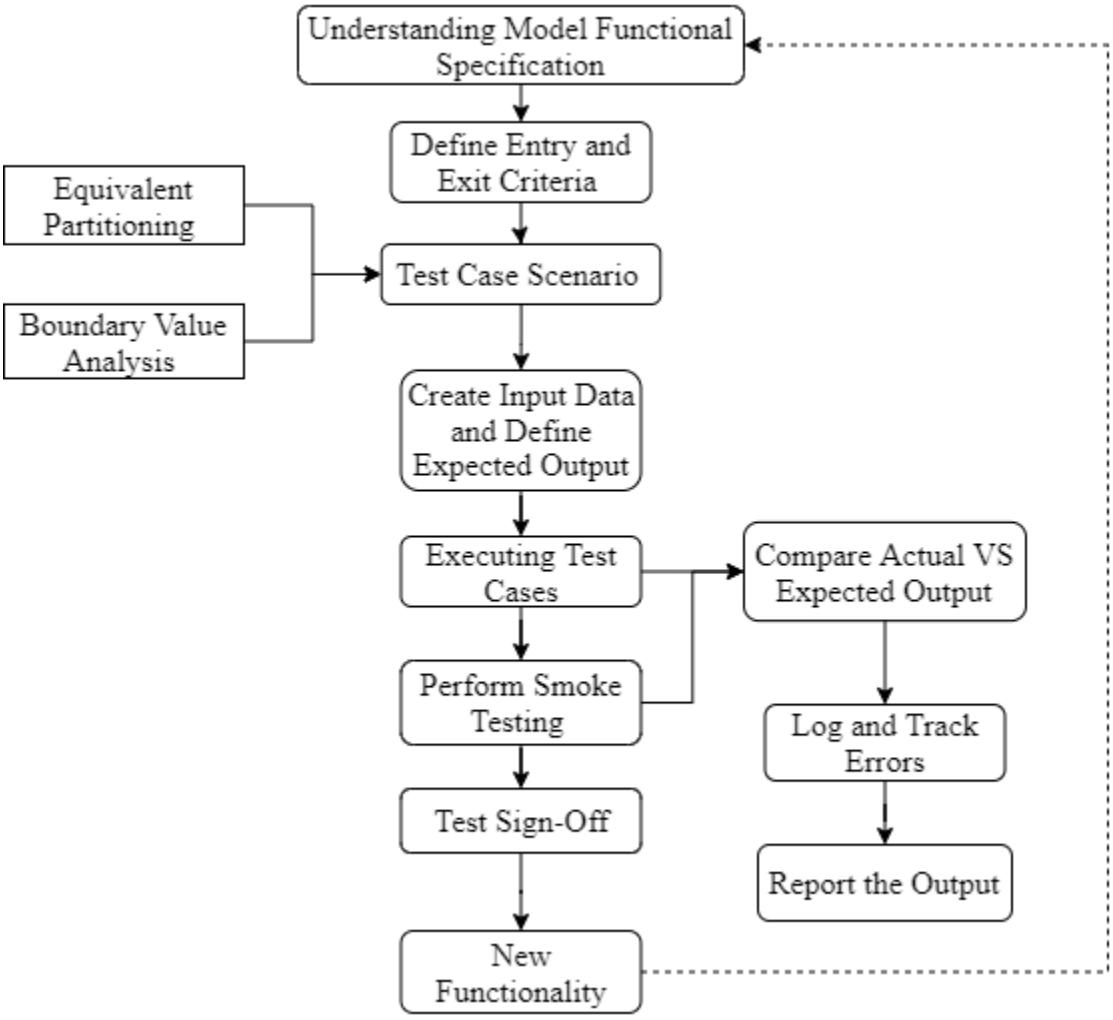
The model evaluation process involved the definition of the model functional requirements. This was in line with the model design (which takes intoaccount the scenarios and the focus group discussion output). The model requirements were defined according to the following criteria: "functionality, completeness, consistency, accuracy, performance, usability, fit with the model, and other relevant quality attributes" as pointed in (Khanom & Miah, 2004). After the entire model requirements had been specified, a test input or test data was identified based on the requirements and grouped into three test cases. An expected outcome was specified with each selected test input value for each test case before computing or running the test case. Thereafter, the test cases were executed and the outcome was recorded per input. In the end, a comparison of the actual outcome and expected results was done and a conclusion was drawn.

3.9.2 Functional Testing Process

The functional testing aimed to address the core purpose of the model and to prove the overall concept of this study. To test and validate the model, this study adopted a guideline described by Shas (2018).

Figure 15

Shas Process for Conducting Functional Testing



The entire steps were, however, not used but the steps were summarized but still kept the process viable. The functional testing process divided the evaluation process into the following steps.

Step 1. Test Goal Definition

The main goal of functional testing was to check how closely the model feature/specification is working as per the specifications. The functional testing goals mainly focused on validation and defect testing. I.e., to demonstrate that the model meets the requirements and to discover the defects in the functionality.

Step 2. Entry Criteria and Exit Criteria Specification

The entry criteria (The beginning) involve the requirement specification, Test Cases preparation, Test data creation, and model setup ready for evaluation. While the exit criteria are when the Execution of all the functional test cases had been completed and no critical P2 bugs are open.

Step 3. Listing The Scenarios to Create Functional Test Cases

This step designed the model test scenarios for the design specification. A `test scenario' is the summary of the model's functionality. Based on these scenarios test cases were prepared.

Here is the list of possible scenarios for our payment gateway example.

i) Users create an account with the model
ii) Users authenticated based on the information provided
iii) Buy stable counts
iv) Transfer stable counts
v) Users can dissolve their crypto accounts
vi) Spend the stable coin
vii) Convert the coin into other cryptocurrencies

Step 4. Definition of Input Data and The Expected Output

Input data for the functionality testing as per the requirement specification was specified. Later from the requirement specification, the output was determined for the functionality under test. The functionalities targeted the following features

i) Payment gateway

ii) Debit/Credit Card Options

iii) API

iv) Swap operation

Step 5. Executing Test Cases

The prepared test cases were executed and the outcome was recorded for comparison as shown in table 11.

3.10 Pilot Testing

Pilot testing is a type of software testing performed by a group of end-users before full deployment (Dellinger et al, 2018). It helps identify the issues related to the various components of a system and helps gauge user experience. It also evaluates the feasibility and performance of the developed research project in real-time conditions. In the view of this study, these pilot study objectives were adopted. It intended to ascertain that the model could help users accomplish all the required tasks. It aimed to get feedback from the potential end-user for present and future advancement. At the end of the pilot testing, a review of the user's feedback and a report is presented in section 4.4.2 and 4.4.3. Any error reported or user experience issues were corrected for improvement.

3.10.1 Pilot Testing Framework

Pilot testing usually depends on the model complexity. This, therefore, means that different models/software have different pilot testing frameworks. For the case of this research, a pilot study framework was proposed by Kallio et al (2016). This framework proposes five different phases of completing a pilot testing; (i) Defining the project and the research, (ii) preparing for the pilot test, (iii) Deploy the pilot testing, (iv), collecting the data and evaluating the pilot test, and (v) prepare the product.

3.11 Ethical Consideration

Boddington (2017`) suggests that researchers need to strike a balance between the pursuits of knowledge on the one hand and the rights of research participants or others in society on the other. There should also be a balance between the potential benefits of the research outcome and its potential costs like loss of dignity, privacy, self-esteem, or democratic freedoms. It is essential that ethical considerations are taken into account in the technology research process (Floridi et al., 2017). According to Boddington (2017), ethical principles should ensure that research participants give informed consent in which participation is voluntary and based on an informed decision. During the research process, the principles of ethics were adhered to to ensure the preservation of participants' dignity and emotions when asking probing questions. These include participant's informed consent, voluntary participation, information confidentiality, and Anonymity.

Through informed consent, the participants were given information about the research and their role explained. Informed consent was obtained through a procedure that was reviewed and approved by Kabarak University Research Ethics Committee (KUREC) as shown in appendix iix. Participants were enrolled to focus groups based on the research comprehension checklist. The comprehension checklist administered is in appendix iii. To ensure confidentiality, privacy, and

data safeguards, any information collected was not be shared. Information about the participants collected was stored and no one but the researcher team was able to see it. No names and identification information were required unless the participant wished to be subsequently provided with a summary of the research outcomes. Any information about the participants had a focus group number and unique ID on it instead of their official name to ensure anonymity. The focus group participant codes (in form of PTID) to label data instead of names and a separate list of code-to-name match-ups is kept. Only the researcher knows what the participant's unique ID or focus group is. It has not and it will not be shared with or given to anyone except the research team. The research ensured that sources for all information of others are acknowledged through complete, accurate, and specific references, footnotes, or use of quotation marks.

The research also followed ethical guidelines, which included an ethics review process before engaging respondents to ensure that procedures were fair and unbiased to all who were involved. Ethical clearance was obtained from Kabarak University Research Ethics Committee (KUREC). The required approval permits were sought from the relevant institutions such as the university and National Commission for Science, Technology, and Innovation (NACOSTI). In this research, the researcher also appended an introduction letter from the Institute of postgraduate and research of Kabarak University

3.12 Conclusion

This research attempts to address the important traits of an optimal cryptocurrency to realize a better crypto-based medium of exchange and a good unit of account in both local and cross-border retail business. It focuses on realizing price stability, scalability, privacy, and decentralization of a crypto asset while maintaining all its blockchain-based features. The projected research aims at increasing and widening the adoption of crypto coins by ensuring simplicity along with the

elegance of concept, easy integration points for partners, and the ability for an exchange to work with. With a huge market cap for cryptocurrency and the presents of digital fiat currency, this research would mutually integrate the popular digital fiat currency into the proposed platform to ensure 1-1 mapping of the fiat currency and the projected crypto-asset. This idea was informed by the fact that cryptocurrencies are there to stay as long as blockchain technology is there. It recognizes that blockchain technologies automatically generate cryptocurrencies to charge the services provided by the system, credit essential services to the system, and of exchanging credits for services. Thus, designing suitable stable coins is essential for the blockchain system to perform financial functions efficiently.

CHAPTER FOUR
DATA ANALYSIS AND RESULTS

4.0 Introduction

This chapter presents the analysis and findings of the study as set out in the research methodology. The general objective of this study was to develop a model for creating stabilized cryptocurrency using fiat currency to enhance global electronic commerce. This was achieved by answering the research questions derived from the specific objectives and application of the specified research methodology. This chapter will first present a summary of the integrative literature review on bottlenecks experienced in using the existing cryptocurrency models used in E-commerce. It will also proceed to provide the model design, implementation, and evaluation.

The integrative review data analysis seeks to address the first objective of the study. The first objective aimed to determine the weaknesses in the existing Cryptocurrency models used in E-commerce. It scrutinizes and identifies the weaknesses in the present collateralized and non-collateralized coins thus guiding the projected model design and implementation.

The analysis of focus group data seeks to find meaning from participants' recorded findings for the questions in the discussion guide. Accordingly, it seeks to identify the proposed model's requirements, and its components to facilitate the model design and implementation. The chapter covers the findings based on the objectives. The findings were then presented in tables, frequencies, figures, and percentages with explanations being given in prose thereafter.

4.1 Weaknesses of Existing Cryptocurrency Models Used in E-commerce

Objective one of the study required a review of the existing cryptocurrency weaknesses that limit its adoption to the current financial setup and usage in the present E-commerce environment. This was achieved through a desk research of literature review and a validation process through expert focus group discussion to interrogate and verify the integrative review results. This methodology

provides a comprehensive, critical and objective analysis of current knowledge on cryptocurrency weaknesses and their causes. Secondary data on various cryptocurrency weaknesses was collected, which is presented herein.

4.1.1 Methodology for the Identification of Weaknesses Existing Cryptocurrencies

A literature review study was carried out to examine and identify the weaknesses of the existing cryptocurrencies. Specifically, an integrative literature review guided by Whittemore and Knafl framework for literature review was used. The following were the objectives of the literature review;

i) To identify cryptocurrency weaknesses if any, within the present e-commerce ecosystem
ii) To identify the various causes of volatility in cryptocurrency

The integrative literature review was premised on the following empirical research questions.

i) To what degree do the cryptocurrency weaknesses within an E-commerce ecosystem contribute to limited adoption?

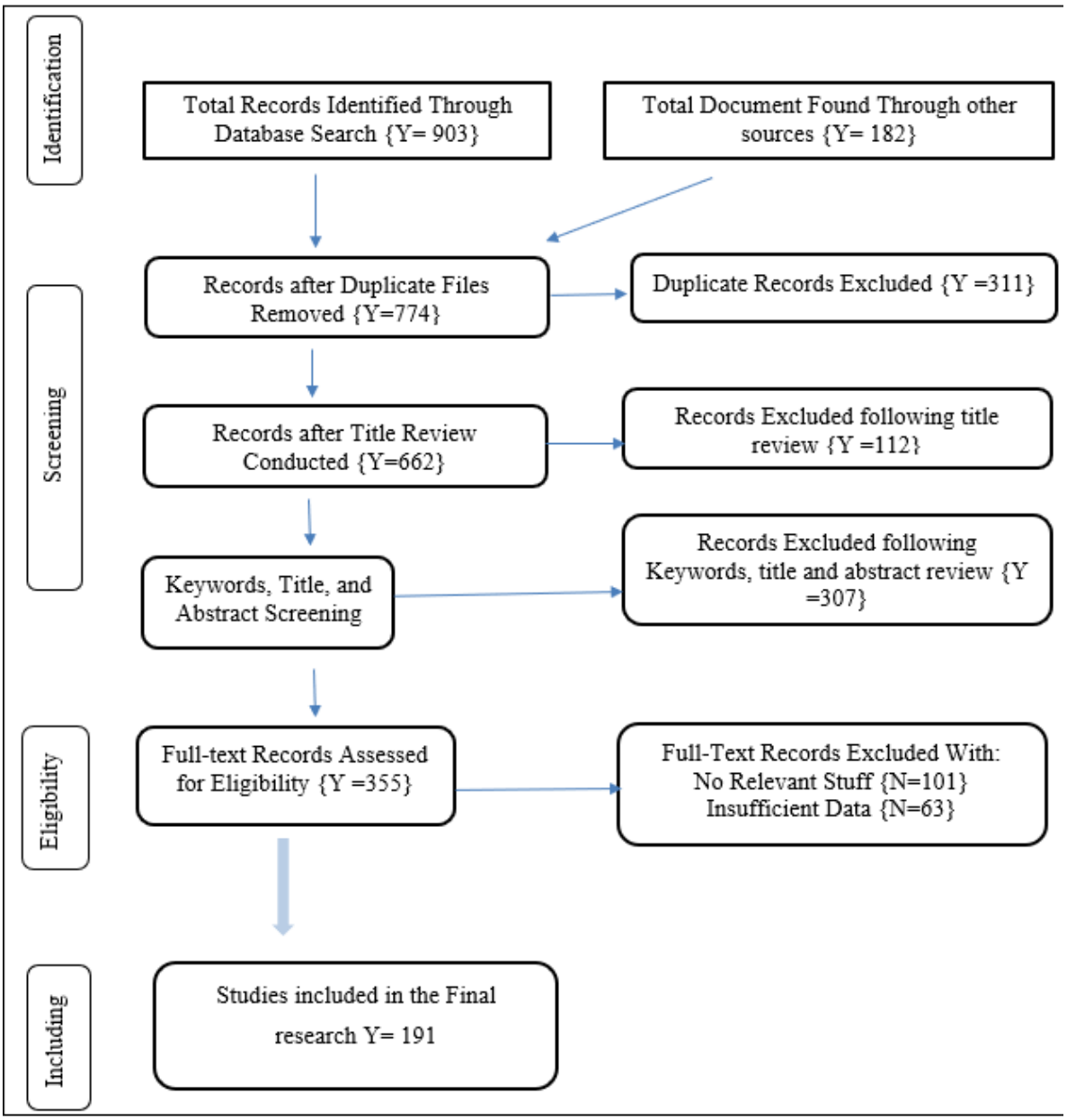
4.1.2 PRISMA Checklist Flow Diagram

The inclusion and exclusion criteria are key components of the integrative literature review. Inclusion criteria are everything, which a study needs to be included in the review. In contrast, exclusion criteria explain the factors, which would make a study ineligible and the study needs to exclude them from the review process. The assessment of multiple Systematic Reviews (AMSTAR) and preferred reporting item for systematic review and meta-analysis (PRISMA) tools are commonly used exclusion and inclusion checklist criteria. According to (Ding et al, 2020), AMSTAR tool is usually used for investigating the methodological quality of a literature review. On the other hand, Brown et al (2020) described PRISMA as a tool that focuses on systematic reviews through evaluating randomized trials, particularly in the evaluation of interventions. The

PRISMA tool provides evidence-based items used for systematic reviews and Meta-analysis. The current study used PRISMA tools for the integrative review because of its importance to demonstrate the quality of reviews, allowing researchers to assess the weaknesses and strengths, and allowing replicating review methods. The PRISMA tool used during this study is given in the diagram below.

Figure 16

PRISMA TOOL & Paper Selection



After deep insight and searching through ACM Digital Library, this study found research articles matching the keywords “volatility and other challenges in cryptocurrencies”. The initial search yielded a total of 903 papers, with 182 additional sources being found outside of the initial search. Out of 1085 selected sources, this review found that 311 research papers were replicated. Other

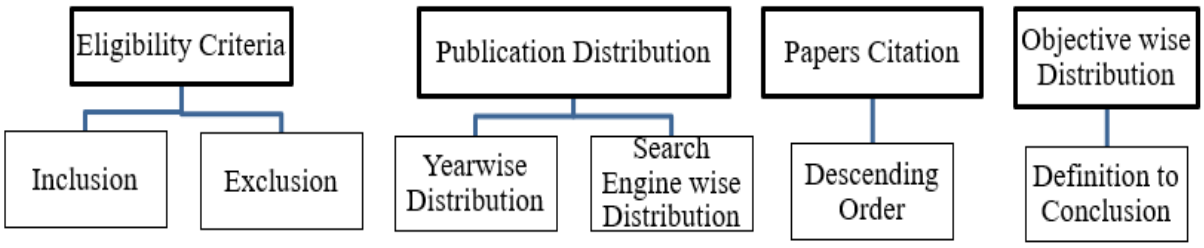
sources were excluded either because of the title, abstract keywords or found irrelevant in the full-text review. For final data synthesis and data extraction, this study considered 191 sources for reviews, and 66 out of 191 were reviewed before reaching theoretical saturation.

4.1.3 Critical Appraisal Skills Program (CASP) Tool

The critical appraisal skills program is a generic tool for appraising or systematically assessing the trustworthiness, relevance, and results of published papers during a qualitative research process (Long et al, 2020). It helps researchers to extract meaning, relevant, and reliable information that exists in literature matching with the current study. For the current study as discussed above, the study relied on keywords and appraisal tools, which match the objectives and theme of the present study. For further elaboration and extracting relevant information, the researcher followed four steps, which guided to completionof the current study task. The figure below shows the steps taken to select the relevant research materials.

Figure 17

Critical Appraisal Skills Program Tool



The eligibility criteria for inclusion and exclusion have been briefly discussed in the research methodology and PRISMA Tool framework. For publication distribution, the current study considered only the research articles that are been published after 2015 and for research journals, the researcher relied on ACM Digital Library academic search database for computer science with

the highest number of articles and bibliographic entries. Paper citations have been considered as key focused, where the study considered only those papers that have more than 10 citations.

4.1.4 Synthesis and Data Analysis

Data synthesis is a statistical measure to combine the results of different studies and literature to obtain a qualitative estimate of the overall effect of a particular variable or intervention on a defined outcome (Ding et al, 2020). It helps researchers to combine the arguments, ideas, findings, recommendations, and critical reviews of different researchers in a systematic manner. In the integrative literature review process of this study, the researcher focused on the arguments, ideas, judgments, and critical reviews of the previous studies related to the first objective of this study.

4.1.5 The Weakness of Existing Cryptocurrency Models Used in E-commerce

The literature review study exposed numerous weaknesses that hinder the adoption of cryptocurrency in e-commerce. The results identified were as follows;

Weakness 1: Highly Volatile

The characteristics of cryptocurrencies are that they have no controlling agency, and the cryptocurrencies market is emerging and still small. They also lack governance are purely digital assets and are not backed by anything physical like a currency or commodity and there are no governments to enforce their use as a currency. This makes cryptocurrencies susceptible to speculative bubbles fueled by irrational speculative activity that leads to a high level of volatility (Moratis, 2021)

Weakness 2: Conversion Issues

Cryptocurrency to cash or one cryptocurrency to another conversion is limited to a few vendors (Katsiampa, 2019). The few vendors that accept conversion also limit conversion monetary value

to a little cash. Many conversion vendors prefer conversion for other cryptocurrencies. This affects the class of cryptocurrency holders that are willing to convert their cryptocurrency to fiat currency.

Weakness 3: Scalability

The generally acceptable country-wise currency exchange and banking transactions in different currencies have been made scalable. Cryptocurrencies however have not reached the scalability level of the present currencies (Lacity, 2020).

Weakness 4: Lack of Legislation

Digital currencies are decentralized virtual entities, and authorities are currently not geared to handle this advanced technology. Therefore, the lack of legislation regulating these digital currencies and providing any sort of user protection has become a huge challenge (Kondo et al, 2020).

Weakness 5: Illiquidity and Trading Costs

In research to evaluate volatility connectedness in the cryptocurrency market, Yi et al (2018) found that the cryptocurrency market is generally less liquid. They indicated that the supply of many cryptocurrencies is controlled, with new units released according to a pre-set timetable, and it should thus come as no surprise that the high volatility of cryptocurrency prices is liquidity-driven. This constrains the ability of investors to exit from their cryptocurrency positions. In their findings also, part of the issue is that there is also no uniformity in the treatment of cryptocurrency trading since some exchanges incorporate the inherent features of cryptocurrencies, while others offer bilateral trading, with some replicating the core features of electronic trading platforms.

Weakness 6: Custody, Clearing, and Settlement Problems

Besides further regulatory clarity, institutional custodial solutions for cryptocurrencies are both legally and technologically complicated. Pandya et al (2019) in their research to investigate cryptocurrency adoption efforts and security challenges in different countries found out part of the complexity is driven by the public and private key management. This research further indicated that the cryptographic keys need to be safeguarded and custodial solutions, therefore, must include multilayered security features that appropriately manage and control how custodial systems can access, use and verify these keys. When these security measures are inadequate, disastrous results can ensue.

Weakness 7: Valuation Difficulties

There is no consensus valuation approach, there are no commonly accepted metrics, and reported pricing information may differ substantively across venues (Schär, 2020).

Weakness 8: Interoperability

The ability of blockchains and cryptocurrencies to see, access, and share information across different blockchains or blockchain networks is still limited (Fauzi et al, 2020). Interoperability enhances transparency and increases the communication rate of blockchains. Presently the technology has been divided to make multiple uses of it in different industrial domains and separate forms of cryptocurrencies. The technology needs to be made interoperable for the internet dedicated to Blockchain and crypto exchange (Pandya et al, 2019).

Weakness 9: Cryptocurrencies are Unpopular

A very small group of online merchants still only accepts Cryptocurrencies. This makes it unfeasible to completely rely on cryptocurrency and blockchain-based tokens as a currency (Dennis & Disso, 2019).

Weakness 10: Regulatory and Legal Dilemmas

Cryptocurrencies are not regulated and do not benefit from the standard legal protections afforded by traded financial instruments. This leads to convoluted legal risks and inserts uncertainty, which can meaningfully influence both instability and risk management for these digital assets (Kang et al, 2021). There is also still no international consensus on how to best regulate cryptocurrencies (Yin et al, 2021).

Weakness 11: Diversity

Cryptocurrencies are qualitatively and technically diverse and incompatible. The various presently existing cryptocurrencies differ in several aspects, especially in terms of security, programmability, and governance characteristics (Valdeolmillos et al, 2019).

Weakness 12: Anonymity

To provide some form of privacy for users in the cryptocurrency ecosystem, cryptocurrencies like Bitcoin have designed their protocols to be pseudo-anonymous, where users use public key addresses to conduct their transactions rather than their actual real-world identities. Pseudonymity results in transactions being recorded as transfers of funds between one public key belonging to the payer to another public key belonging to the payee, thus preventing an observer from identifying the real-world identity of the payer and payee (Mnif, & Jarboui, 2021). However,

complete anonymity opens the door to illicit activity that by definition cannot be investigated (Vukolić, 2015)

Weakness 13: The Technology Is Still Immature

According to Hughes et al (2019), cryptocurrencies are facing implementation obstacles beyond the lack of regulation and inactive obligations. The cryptocurrency and blockchain technology is an emerging one and is still immature in an ecosystem where other options are widely scalable and accepted over it. Kaur and Kaur (2020) also indicated that however long cryptocurrency technology has existed, not much has been done to expand it or enhance interoperability and legal use cases.

Weakness 14: Legal Obstacles

In addition to the lack of legislation, the other big obstacle that stands in the way of cryptocurrency holders like Bitcoin traders and users is the challenge to spend their holdings (Sharma et al, 2020).

Weakness 15: Usability

While cryptocurrency promises that it's accessible and decentralized, its complexity is restricting its user base to a narrow, homogeneous set of early adopters. According to Qureshi et al, (2020), Usability is one of the huge obstacles that hinder the cryptocurrency's path to mainstream adoption.

Weakness 16: Bad Imagery

The cryptocurrency industry association with shady business practices, high-profile hacks, environmental challenges, speculation, market manipulation, criminal associations, and a pronounced lack of regulatory clarity have created a perception and image problem (Bez et al, 2019).

Weakness 17: Data and Modeling Obstacles

There is no necessary data to model the future of cryptocurrencies. The detailed but narrow data set of actual transaction prices that cryptocurrency markets provide is inadequate for modeling purposes (Teker et al, 2020).

Weakness 18: Expensive Mining Process

Cryptocurrency mining is energy-intensive and makes the mining process to be expensive. The amount of electricity used to mine bitcoin according to Bouri et al (2019) has historically been high compared to any other usage in most countries.

The results of this analysis as shown above indicated that there are several weaknesses in the present cryptocurrencies. To enhance visualization and interpretation, the 18 weaknesses are briefly described and presented in the matrix Table 3 below. The frequency to show several sources that mentioned each weakness and the percentage concerning all reviewed papers before reaching theoretical saturation. Although research shows that Distributed Ledger Technology (DLT) and cryptocurrencies open up many opportunities, such as fast, efficient, traceable, and secure local and cross-border transactions, the above challenges must be addressed. Since it is at least difficult if not complex to consider all weaknesses at once, this research focuses on the critical weakness with the highest weight (cryptocurrency volatility) and by extension, it solves some and not all of the other weaknesses.

Table 3

Cryptocurrency Weaknesses Derived from The Literature

SN	Cryptocurrency Weakness	Description	Weight out of 66	Percentage mentioned
1.	Highly Volatile	Cryptocurrency prices are highly volatile, responding strongly to global events and speculative concerns about the cryptocurrency market.	66	100%
2.	Conversion Issues	Conversion remains a huge hurdle for Bitcoin vendors. As Bitcoin is not a fiat currency and is only limited to monetary value when converted to a cash equivalent, not many vendors go for its conversions for other cryptocurrency types.	61	92.42%
3.	Scalability	Cryptocurrencies are less scalable	59	89.39%
4.	Lack of Legislation	Digital currencies are decentralized virtual entities. They are purely digital products, and authorities are currently not geared to handle this advanced technology. Therefore, the lack of legislation regulating these digital currencies and providing any sort of user protection has become a huge challenge.	52	78.79%
5.	Illiquidity and Trading Costs	The cryptocurrency market is generally less liquid	51	77.27%
6.	Custody, Clearing, and Settlement Problems	Institutional custodial solutions for cryptocurrencies are both legally and technologically complicated.	49	74.24%

7.	Valuation Difficulties	There is no consensus valuation approach, there are no commonly accepted metrics, and reported pricing information may differ substantively across venues.	45	68.18%
8.	Interoperability	The technology needs to be made interoperable for the internet dedicated to Blockchain and crypto exchange.	41	62.12%
9.	Cryptocurrencies are Unpopular	The willingness of parties to accept the cryptocurrency as a standard of value in their mutual dealings is still an issue	32	48.48%
10.	Regulatory and Legal Dilemmas	cryptocurrencies are not regulated products and do not benefit from the standard legal protections afforded traded financial instruments.	27	40.91%
11.	Diversity	Cryptocurrencies are qualitatively diverse and not interchangeable (cryptocurrencies differ)	25	37.88%
12.	Anonymity	A problem for combating money laundering and countering terrorist financing or tax evasion	20	30.30%
13.	The Technology is Still Immature	The technology is emerging and still immature in a system where other options are widely scalable and accepted over it.	20	30.30%
14.	Legal Obstacles	In addition to the lack of legislation, the other big obstacle that stands in the way of cryptocurrency holders like Bitcoin traders and users is the challenge to spend their holdings.	19	28.79%
15.	Usability	Buying and selling cryptocurrencies currently are difficult	15	22.73%
16.	Bad Imagery	Cryptocurrency still has a PR problem.	12	18.18%

17.	Data and Modeling Obstacles	The detailed but narrow data set of actual transaction prices that cryptocurrency markets provide is inadequate for modeling purposes.	09	13.64%
18.	Mining Process	The mining process in cryptocurrencies takes up more electricity bills	03	4.55%

4.2 Model Design

This section presents the results of objective two of the study, which set out to design a stabilized cryptocurrency model for global electronic commerce. The design was based on the findings of the first objective of the study as presented in section 4.1 (specifically cryptocurrency volatility) and the focus group discussion findings. It begins with defining the design philosophies and objectives that guided the design process. The model functional and system requirements are also presented.

4.2.1 The Design Philosophy and Objectives

The principal objective of the Central Bank of Kenya is the formulation and implementation of monetary policy directed to achieving and maintaining stability in the general level of prices (CBK) (The Central Bank of Kenya, 2022). This aims to achieve stable prices measured by low and stable inflation and to sustain the value of the Kenya shilling. In driving this core objective, the design principle for the stable cryptocurrency in this research also delivers on key economic objectives of the Central Bank of Kenya to positively affect overall economic growth and to generate significant social and economic benefits for all. The design aimed to realize a cryptocurrency that would enable households and businesses to make fast, efficient, and reliable payments while benefiting from a resilient, advanced, inclusive, and competitive payment system.

4.2.2 Design Philosophies

The design philosophies encapsulate the overall objectives of the envisioned model. The philosophies outline the model'spurpose to act as a medium of exchange and as a payment system. The model design was also based on three mutual principles advocated by the Bank for International Settlements (BIS); do no harm, co-existence, and Innovation and Efficiency (Westermeier, 2018). With respect to the first principle, the envisioned cryptocurrency should in no way impede or interfere in the ability of financial institutions to carry out their pursuit or affect the present mechanisms to ensure monetary and financial stability. Secondly, the envisioned cryptocurrency should be able to coexist with different forms of money already in use. The existing forms of money such as cash, reserves, and settlement accounts should complement each other and coexist. Lastly, the cryptocurrency design should be open to innovation and efficiency.

Based on these principles from the Bank for International Settlements and the principal objective of the Central Bank of Kenya, this study developed six philosophies that guided the model design. These are Inclusivity, Innovation, Efficiency, Resilience, and Coexistence.

Table 4

Model Design Philosophies

Philosophy	Description
Inclusivity	The envisioned cryptocurrency should foster the inclusion of all in the financial system and enable access to financial services.
Innovation	The envisioned cryptocurrency will provide a platform that fosters continuous innovation and collaboration across different sectors of the economy
Resilience	The envisioned cryptocurrency will strengthen the existing payment system by serving as a key alternative means for digital transactions in the country and across the border.
Coexistence	the envisioned cryptocurrency should be able to coexist with different forms of money already in use
Efficiency	The envisioned cryptocurrency will enable fast and efficient payments, reduce transaction and setup costs, and widen direct participation in the payments value chain.
scalability	The model should be scalable and accommodate future trends and financial ecosystem needs

4.2.3 Design Dimensions

The model design adopted two dimensions. (i) Analysis of potential model business environment to realize services necessary for users. The deliverable is the model functional requirements (the potential processes that the system has to perform as a part of supporting a user task)**.** (ii) Analysis of the model functional requirements to define system requirements necessary to build a model that can deliver the required user needs.

4.2.4 Model Functional Requirements

The model functional requirement describes what functionality should exist in the system to support an activity that the user would like to achieve. It communicates the model's expectation from an end user's perspective. To achieve the functional requirements, the focus groups and scenario-based design methodologies described in the methodology section were used.

4.2.4.1 Framework for Scenario-Based Design

The model designwas inspired by metaphors and technology options to realize a minimum viable product to demonstrate the viability of the overall research idea. As indicated earlier, at the center of the overall design were scenarios created through FGDs. The scenario was to describe a specific target user trying to achieve a specific goal or perform a specific task in a specific context. Each set of scenarios had a claim and a narrative. A claim analyzed the possible positive and negative consequences of the key design features. This reflected the usage implications of the design ideas during and after development. While the narrative served as a test case for analytic evaluation and claims hypothesized usability outcomes for one or more test cases.

4.2.4.2 Functional Requirements Analysis

Requirement analysis, also known as Requirement Engineering, is the process of defining user expectations for new software under development (Jayatilleke & Lai, 2018). The primary concern of the study was to develop a model for creating stable cryptocurrency using fiat currency to enhance global electronic commerce. In the SBD, this research expressed an initial analysis of requirements as a root concept (Table 4). The root concept enumerated key aspects of the model's starting vision. This served as a primary guide for further analysis and elaboration of the model'sfunctional requirements.

Table 5

The Root Concept

Component	Contributions to the root concept
High-level vision	The model users to access the stable cryptocurrency
Basic rationale	The stable cryptocurrency overcomes voltility challenge exhibited by the previous cryptocurrencies
Stakeholder:	Convenient access to expected services for users and stakeholders with minimal latency while achieving the model's expected functionality and design philosophy
Starting assumption	Open-ended participatory design process

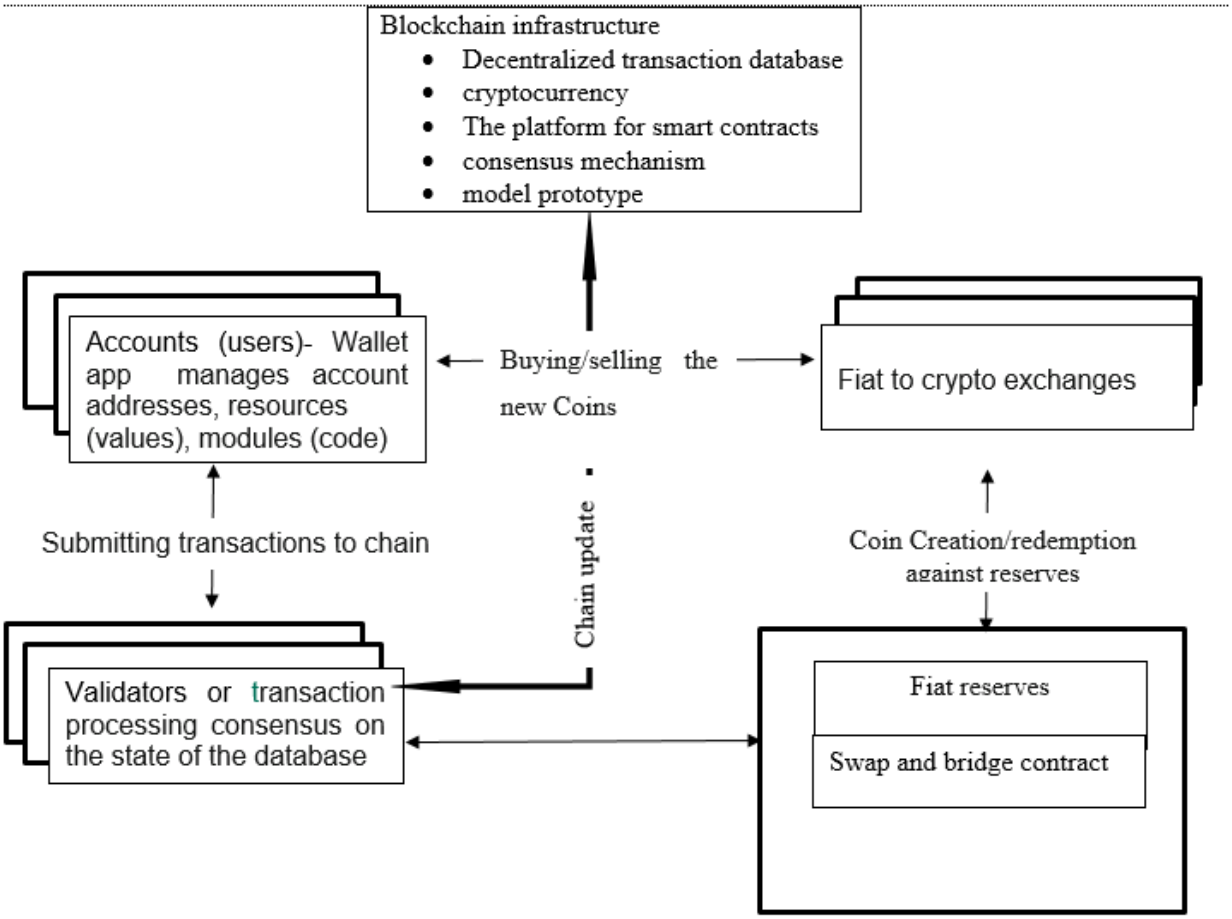
The root concept laid the groundwork for analyzing the model user activities and consequently deriving the model user and system requirements. Although the scenarios were through the expert focus groups, from here henceforth this document will be focusing on analyzing and developing model requirements using the SBD technique. The SBD through the focus group discussions expanded the root concept based on the problem scenarios and claims to realize comprehensive model requirements. A problem scenario is a narrative of current practice that synthesizes actors, themes, relationships, and artifacts Rosson & Carroll (2009)

The generation of problem scenarios started with a description of a set of realistic hypothetical model users, their tasks, and context. This formed the basis for describing and later transforming current activities into system and user requirements. A more systematic evaluation of the scenarios was obtained by asking questions about the scenario that are guided by cognitive and design philosophies. The analysis was also extended through “what if” reasoning that explored other possible requirements.

During the design process the model design was expected to contribute to the credibility of the new cryptocurrency as a unit of account, a stable medium of exchange, and finally as a store of value. Hence, the new cryptocurrency design fulfilled the basic functions of money. Users have to purchase and sell the stable cryptocurrency through the model. The model is linked to fiat reserves and supports the exchange of the cryptocurrency from one form to another. Various forms of fiat currencies shall be accepted (mobile money, electronic exchanges, and mobile banking for the current POC). The future model advancement will however accept more interaction as indicated in the design philosophies. The blockchain infrastructure will allow quickly and securely transactions executions. This will be possible through cryptographic technologies and algorithms that ensure consensus among the network nodes. It will maintain the model integrity by preventing double spending of monetary units while ensuring that other DLT features are enjoyed within the model operation. The figure below describes the model features abstractly.

Figure 18

Abstract Model Features



To describe the various functional requirements that users, user stories from the model abstract and scenarios described during the focused group were written as shown in the table below. The tasks and contexts thereafter were defined in detail. An effort was made to simplify the user stories and requirements to the bare minimum, while still keeping the PoC at a viable level of usability and security.

Table 6

User Stories Defining Functional Requirements

As a...	I want to. . .	Traceability
User	Be able to automatically generate my cryptographic identification parameters	1.1
	Be able to create an account with model	1.2
	Use memorable parameters for authentication	1.3
	Be identified cryptographically	1.4
	Be able to see my cryptographic transaction records	1.5
	Make withdrawals from my cryptocurrency account	1.6
	Transfer cryptocurrencies currencies from my wallet to another wallet	1.7
	convert my cryptocurrency to other forms of currency	1.8
	pay for goods and services using my cryptocurrency	1.9
	Deposit cryptocurrency (create cryptocurrency by depositing fiat currency)	1.10
	To manage my account /wallet (check address and balance)	1.11
Admin	Be able to automatically generate my cryptographic identification parameters	2.1
	Be able to create an account with model	2.2
	Use a memorable parameter for authentication	2.3
	Be identified cryptographically	2.4
	Be able to view the model users (registered users and access the name service)	2.5
	Be able to view the model cryptographically recorded transactions	2.6
	Be able to access and view the minting records (a record of total/all generated cryptocurrency)	2.7
	Administrate (set up and maintain accounts) the system.	2.8

Be able to view the total burned cryptocurrencies (cryptocurrencies that were permanently removed from circulation as a result of withdrawal or account dissolution)	2.9
Be able to view the total market capitalization for the stable cryptocurrency (Total cryptocurrency in circulation)	2.10

Summarization of the above user stories gives the following model functional overview as shown in the table below.

Table 7

Description of The Model Functional Requirements

The Model Functionality and Functionality Traceability (FT)		**How to realize the target user story(TUS)**	
Functionality	**FT**	**How to realize**	**T.U.S**
1. **User Registration**	A.	All users are required to register with the model before accessing any of the model functionality. This is to capture the user's personal information and authentication details.	1.1, 1.2, 1.4, 2.1, 2.2, 2.3, and 2.4
2. **User Authentication and Security**	B.	The model ensured that all users registered before allowing them to access the model functions. The registered persons are required to log in using a memorable parameter of biodata	1.3, 1.4, and 2.4

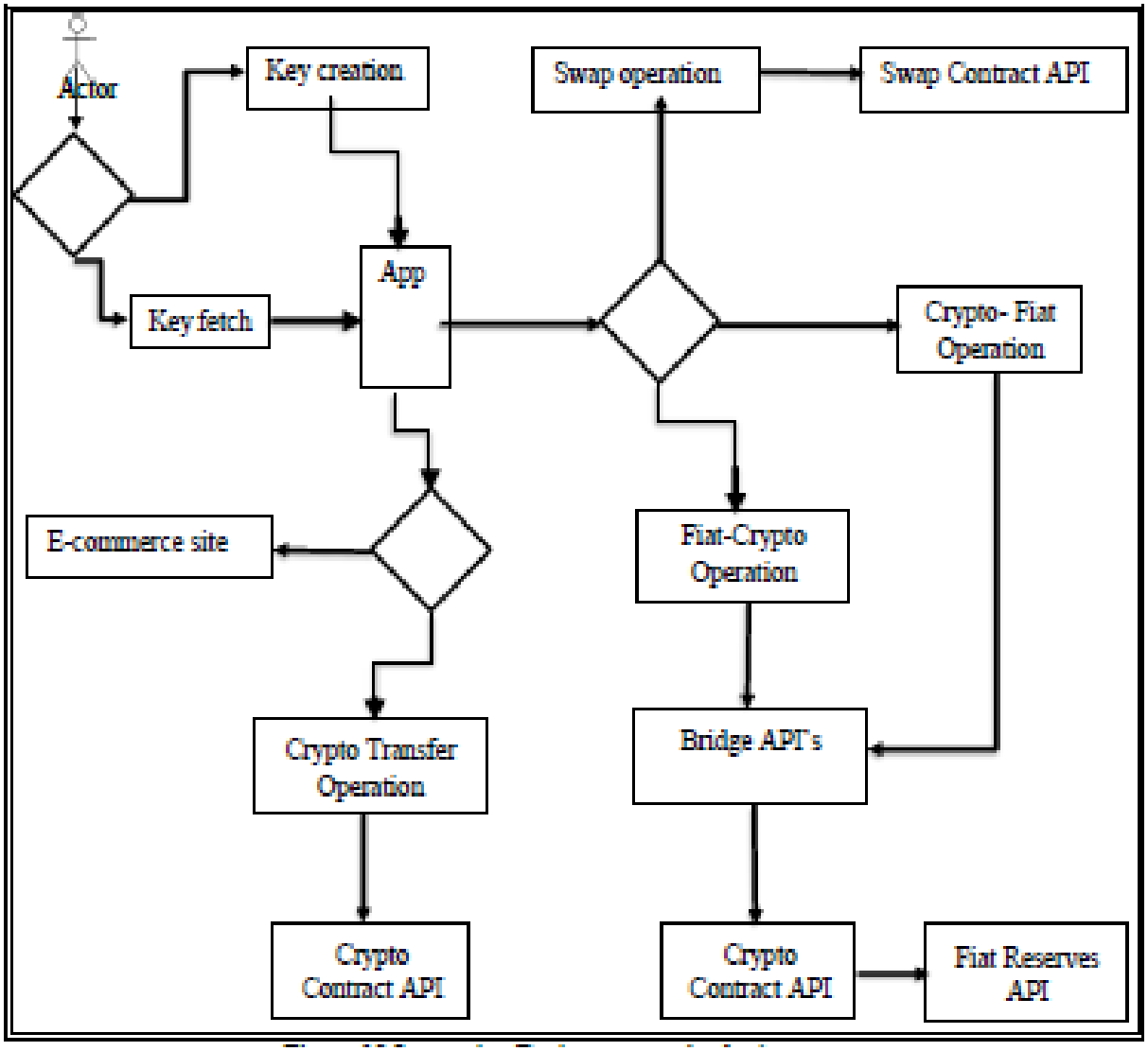
3.	**Stable Coin Creation**	C.	The model created a stable cryptocurrency equivalent to the fiat currency deposit	1.10
4.	**Cryptocurrency Account Liquidation**	D.	The model allowed users to withdraw cryptocurrencies from their wallets.	1.6
5.	**Cryptocurrency Transfer**	E.	The model allowed users to transfer their stable cryptocurrencies from one account to another. This assumed that users would need the transfer module to pay a debt, make a donation or pay for service	1.7 and 1.9
6.	**Cryptocurrency Exchange**	F.	The model allowed users to exchange cryptocurrency from one crypto to another within the liquidity pool	1.8
7.	**Transaction records management**	G.	The model allows the recording of the transaction on the blockchain	1.5, 1.11, and 2.6,
8.	**Report generation**	H.	The model enables users to generate reports regarding transactions.	1.5, 2.7 2.9, and 2.10

4.2.4.3 Interaction Design

The User interaction design shows the activities and tasks that users can perform while using the model. It intends to support the identification and exploration of design alternatives to meet the requirements revealed by analyses of opportunity space and context of use above. It also aids in realizing technical requirements and issues that need consideration to complete the model development.

Figure 19

Interaction Design



4.2.5 Model System Requirements

The model system requirement describes the technical requirements. It designs the technical system blueprint that satisfies the system's user requirements. It also clarifies the system-implementation techniques to deliver the model's functional requirements. In designing the model system requirements, this research has taken into consideration four key design elements based on the recommendations from the World Economic Forum and Bank of International Settlement (BIS) on digital currency implementation as they align with the overall objective of the envisioned model.

4.2.5.1 The Model Design Elements

Based on the model functional requirements discussed in section 4.2.4, the model system requirements include the following design elements; Architecture, Infrastructure, Interlinkages/ interoperability, and Access.

1. The Model Architecture / Reference Model

The model design targeted a platform that incorporates the design philosophies. The model entailed building a technology platform as well as leveraging the existing structures and roles in the payment system to deliver additional value for users. It aimed at realizing a platform that serves as a payment platform on which the users and payment service providers can innovate and create layered payment services to enable broad use cases.

To realize the defined model design philosophies, four key basics were provided:

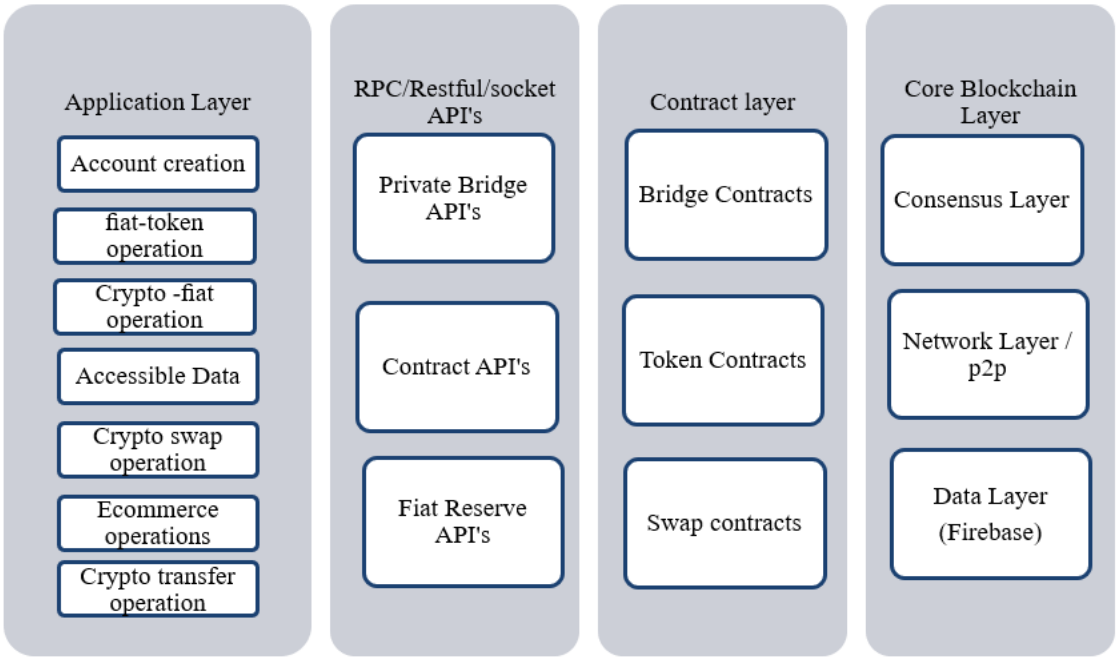
1. A service suite and human-model interaction layer to facilitate interaction between humans/ users and model for service access.

2. Inter-process communication layer to facilitate communicationmechanism between users and the underlying or the model components if an event has occurred or the transferring data from one component to another.
3. Contracts module to execute user requests and respond to events to accomplish specific user requirements
4. A core ledger to serve as the model core and a platform to record transactions and payments to be processed

As a result of the above four essentials, the model was designed to have a four-tiered/ layered architecture; Application Layer, RPC/Restful/socket APIs, Contract layer, and the Core Blockchain Layers. This architecture describes four layers that the model used to realize its operations. In addition, with these four elements, the model core drives inclusiveness, innovation, coexistence, scalability, originality, and interoperability as the baseline requirements and the design philosophies.

Figure 20

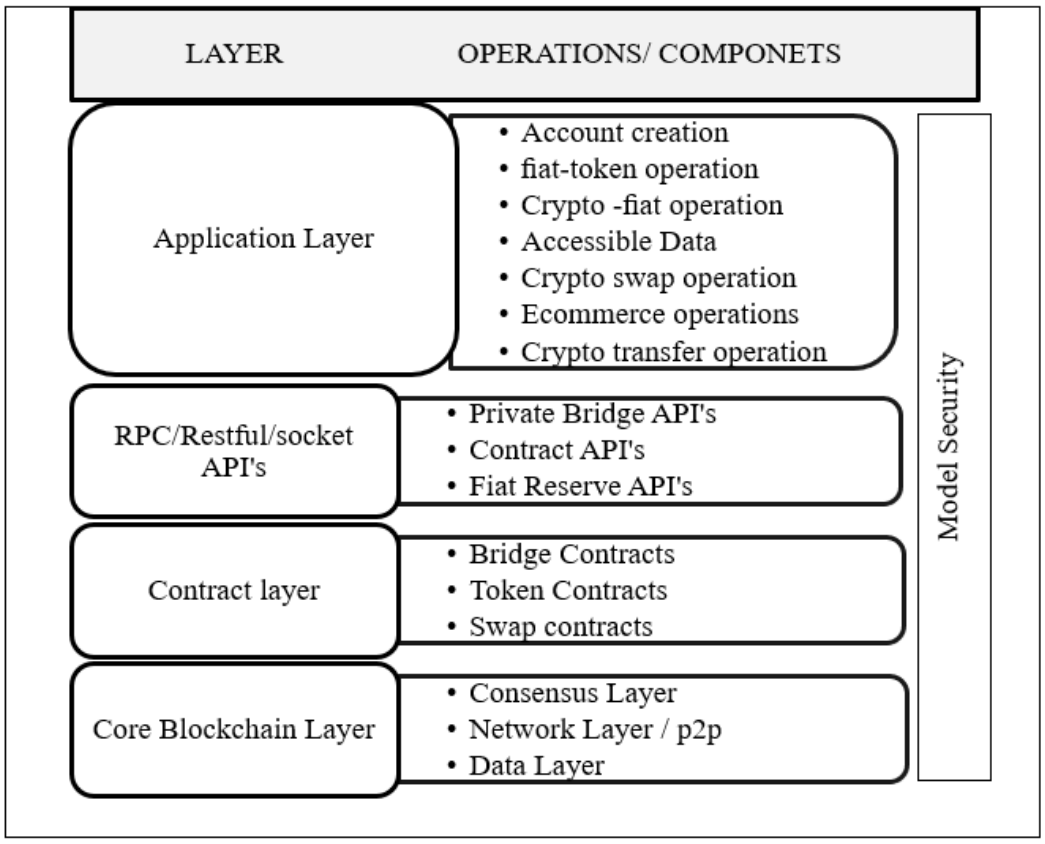
Model Architecture Layers



The four layers above were represented in an abstract framework or domain-specific ontology. This forms the model's reference model consisting of all the elements in an interlinked manner to encourage clear communication.

Figure 21

The Model Architecture / Reference Model



Application Layer

The application layer provides human-model interaction and user service access points. The services include and are not limited to the list provided in the table below as it leaves room for scalability, adaptability to future needs, and further innovation.

Table 8

The Application Layer of Model Architecture / Reference Model

Application Layer Service	Description
Account creation	This service allows to register with the model prior to accessing any of the model functionality. This is to capture the user personal information and authentication details as a requirement for Knowing your customer (KYC)
fiat-token operation	This service will be facilitating conversition of fiat currency to cryptocurrency by invoking the bridge smart contracts
Crypto -fiat operation	This service will be facilitating crypto to fiat currency conversion or liquidation service using bridge based smart contract or Blockchain oracles
Crypto swap operation	Provide cryptocurrency conversion (ie. crypto A to crypto B). in this research, swap operation helps to convert the created cryptocurrency from kenya shilling to other currency like USD.
Crypto transfer operation	This service facilitates transfer of the created cryptocurrency from one account to the another
Ecommerce operations	This operation facilitates electronic payment for goods and services
Accessible Data	Distributed data access by the network crews is facilitated by this service

RPC/Restful/Socket API's Layer

This layer provides a set of protocols and APIs that the clients use to interact with the blockchain network. The model users can query the blockchain-related information such as block number,

blocks, or node connection and send the transaction request within this layer. Remote Procedure Call (RPC), RESTful API, and socket API used in this model operate on this layer. The following are the components that make up this layer for this model.

Private Bridge API - This cross-chain private bridge enables users to transfer crypto-assets or data between different blockchain networks.

Contract API - This API facilitates smart contract communication. It allows contract-to-contract communication and service-to-contract communication.

Fiat Reserve API - This API facilitates the model components to communicate with the Fiat Reserve/ custodian entities. Ideally, it facilitates communication with the M-Pesa business account and the GT-bank account used in the developed model to prove the overall concept.

Contract Layer

This layer defines the Smart contracts used in this model. To classify the contracts, "The Five Types Model" described in chapter three was used. The major smart contracts include Bridge contracts, Crypto Contracts, Swap contracts, and data contracts, Name system contracts. Bridge Contracts connect blockchain to external systems using blockchain oracles to enable smart contracts to execute based upon inputs and outputs from the real world. The Crypto Contracts facilitate the cryptocurrency transfer from one account to another. It contains a map of account addresses and their balances. The Swap contracts facilitate the cryptocurrency conversion from one form to another.

2. Infrastructure

The model infrastructure used was based on the distributed ledger technology (DLT) that would support the adopted four-layered architecture. It also took into account the core requirements of

financial systems and quality attributes which include: user identification based on underlying identity frameworks, high transaction throughput performance, low latency of transaction confirmation, and privacy and confidentiality of transactions and data about the business transactions

3. Access

Financial inclusion was a core objective of this study as highlighted in the design philosophies. To ensure inclusive access while also ensuring the integrity of the financial system, the account based on the mobile money model was chosen for the envisioned cryptocurrency. This mirrors the progress made by the National Financial Inclusion Strategy (NFIS), which plays a significant role in driving financial inclusion by leveraging last-mile networks to identify users and provide banking services through channels such as USSD. With this, the model seeks to enable access by leveraging the existing identity infrastructure in such as the registered phone numbers to identify individuals. A phone number to cryptographic key mapping simplifies the identification mechanism. This identity mechanism will help ensure a robust KYC framework positioned to enable access for all users.

4. Interlinkages/ interoperability

The envisioned cryptocurrency has broad use cases beyond the domestic market as it has the potential to avoid fragmentation and promote global cooperation in the long term as well as support a more connected and inclusive world. Interoperability between the envisioned and other cryptocurrencies has been factored into the overall design. This will help drive the business case for cross-border payments and could potentially address issues of dollarization of the economy, which is a key issue,in those sub-Saharan African countries.

4.3 Model Development

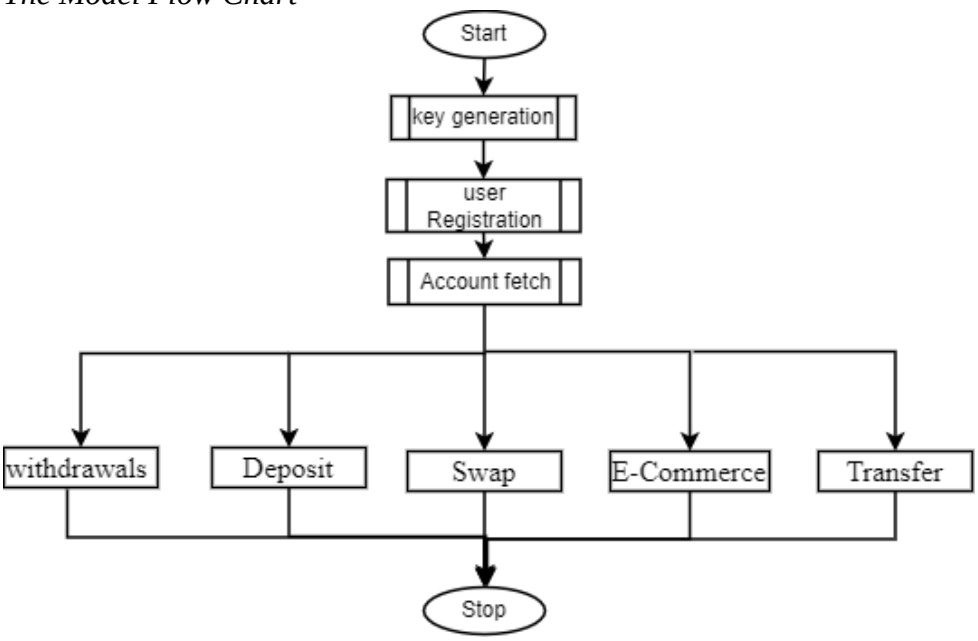
This section demonstrates the attainment of research objective three of the study, which required the researcher to develop a model POC. The model creates a cryptocurrency that complements the existing payment options available. For the current proof of concept, a mobile app that supports the potential user needs identified during the SBD was implemented while leaving room for further improvement and innovation as indicated in the design philosophies. It will offer a broad range of services that will expand as adoption arises and new use cases and other potential functionalities are developed in the future. Although not all the services will be available in the POC, however, the model has limitless possibilities to deliver value, fast, efficiently, and at little to no cost to users.

4.3.1 System Objectives

Based on the model functional requirements specified in section 4.2.4, the overall function to realize the minimum viable product in this research is represented in the flow chart below.

Figure 22

The Model Flow Chart



4.3.2 Development of User Registration and Authentication

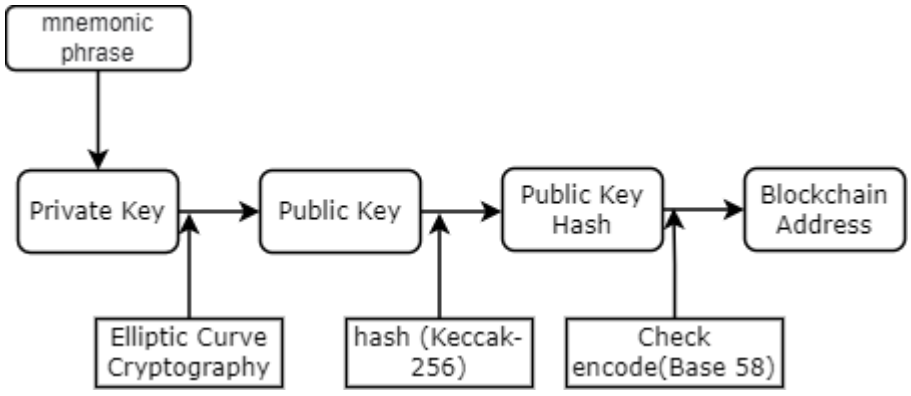
Registration creates a new user account with a record that describes a user and provides proofof identity. To authenticate involves providingevidence that your identity matches the one described in your user account. To be able to register some prerequisite operations described below must be met.

4.3.2.1 Cryptographic Key and Address Generation

For identification within the blockchain domain, it requires a unique address. The unique address or identifier serves as a virtual location or a wallet for sending and receiving cryptocurrency. The address is created by following the steps shown in the figure below

Figure 23

Cryptographic Key and Address Generationflow Chart



The model wallets implement Bitcoin Improvement Proposal (BIP) 39 to define a formula forgenerating mnemonic sentences (also referred to as mnemonic words, seed phrase, or recovery phrase) andthe seed from that mnemonic sentence. That seed is used to produce the private and public keys. The private key generation uses pseudo-random number generators (PRNG) with enough entropy. The private key is randomly selected from the integer space 2^{256}-1 (any number

can be a private key as long as it is within the value of 1 and 2^{256}-1). The role of a private key is to sign a transaction and to create a signature for source authentication against the user address. This, therefore, requires that the private key should be stored securely.

An Elliptic Curve Cryptography (ECC) generates a public key from the private key. The blockchain addresses are unique identifiers that are derived from public keys or contracts using a cryptographic hashing algorithm/ function. A cryptographic hash function is a one-way hash function that maps data of arbitrary size to a fixed-size string of bits. The design and implementation of this model used the Keccak-256 cryptographic hash function. The least (the last 20 bytes) significant bytes from the hashed value form the blockchain address. This is realized using the check encode function (base 58). A prefix 0x in the addresses indicates they are hexadecimal-encoded.

Figure 24

Cryptographic Key and Address Generation

Listing 1: Cryptographic key and address generation

```
//Generating randomness
export default async function generateMnemonic()
export default async function generateMnemonic() {
   let bytes = await Random.getRandomBytesAsync(16)
   let Entropy  = bytesToHex(bytes)
   return Entropy
}
function bytesToHex(bytes) {
   for (var hex = [], i = 0; i < bytes.length; i++) {
     hex.push((bytes[i] >>> 4).toString(16));
     hex.push((bytes[i] & 0xF).toString(16));
   }
   return hex.join("");
}
   const generateAccount = async () => {
       let Mnemonics  = await generateMnemonic()
       const mnemonic = bip39.entropyToMnemonic(Mnemonics)
       setMnemonic(mnemonic)
      //
  }
```

4.3.2.2 User Registration

User registration allows users to create profiles or accounts with the model. All users are required to register before accessing any of the model functionality. This allows users to personalize their accounts and profiles. Utmost care is taken at the entry point of the model to ensure the details of particular users are secured. The user registration is preceded by the prerequisite operations described above.

Figure 25

User Registration Flow Chart

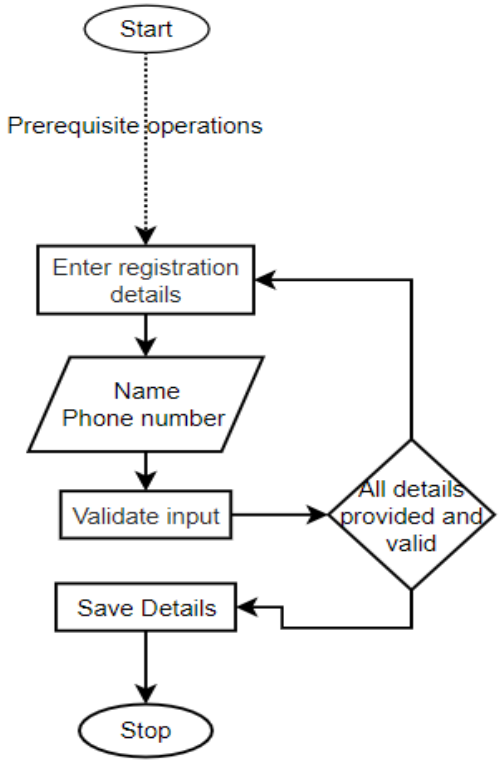
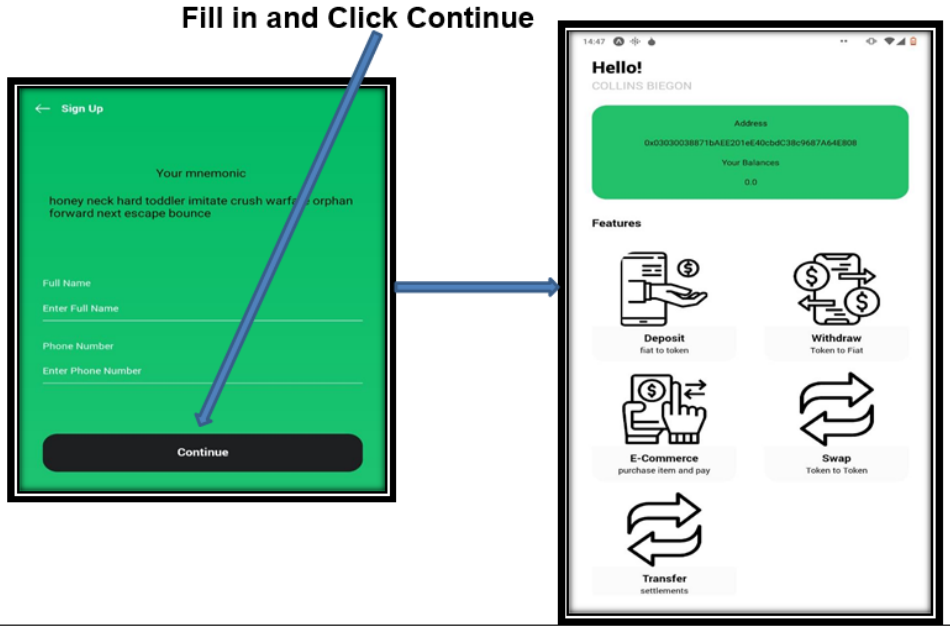


Figure 26:

User Registration



Listing 2: User Registration

```
FrontEnd
export const  setEns = async (details,mnemonic,phoneNumber) =>  {
    const wallet = ethers.Wallet.fromMnemonic(mnemonic)
    const signer = new ethers.Wallet(wallet.privateKey,Provider)
     const phNumber = ethers.utils.parseEther(phoneNumber)
    let message = await contract.metaHash(details)
    const signature = await signer.signMessage(ethers.utils.arrayify(message))
    const tx = await  contract.registername(details, phNumber,signature)
    await SecureStore.setItemAsync('mnemonic',mnemonic)
    return  tx.wait()}
//backend
   function registername( string calldata name, uint256 _No ,bytes memory signature) public {
       bytes32 meta_Hash = metaHash(name);
       address signer = getSigner(meta_Hash,signature);
      ens[signer] = name;
      phoneNumber[_No] = signer;
       users.push(signer);
  }
```

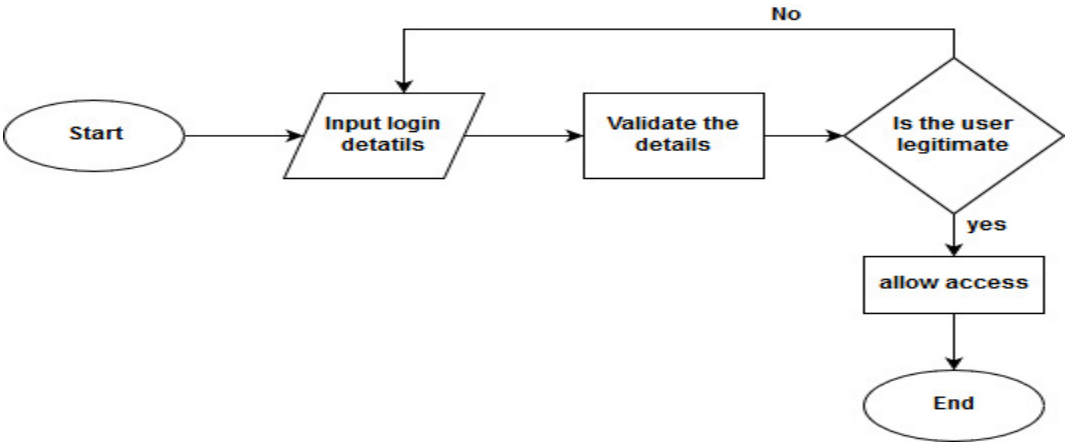
4.3.2.3 User Authentication

The user authentication process provides a mechanism of providing evidence that the user's identity matches the one described in the user account. This ensures that the system users are identified in a cryptographically secure manner so that no unauthorized entities can access the network. The authentication process is shown in the figure below. DLT uses a cryptographic mechanism to ensure unique user and contracts authentication. It uses a 20-byte hexadecimal address to serve this purpose. This, therefore, is not easy to memorize, and this research considered it. To enhance usability and improve user experience, the user details provided during registration

are mapped with the account address to ensure that users can only log in with a memorable parameter. This reduces the mental efforts and challenges that come with human cognition.

Figure 27

User Registration Cryptographic Key and Address Generation

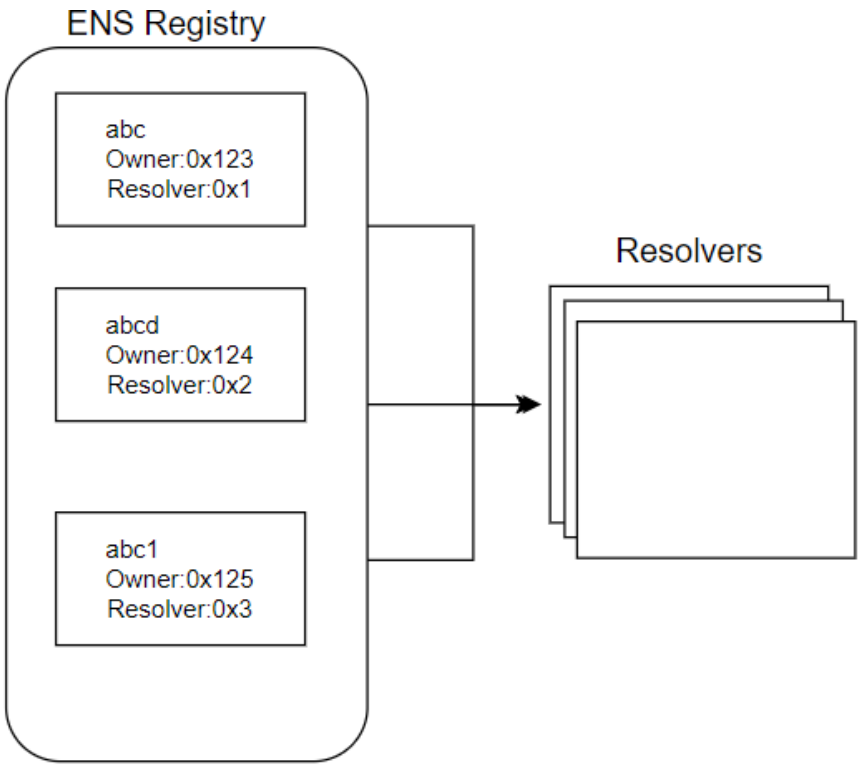


4.3.2.4 Address Mapping

Blockchain addresses are hexadecimal numbers, identifiers derived from the last 20 bytes of the Keccak-256 hash of the public key. This is difficult to memorize and thus a more recognizable and easy mechanism is paramount. In this model, an Ethereum Name Service (ENS) blockchain protocol was used. This ensured that user could use their own unique and memorable user information within the model for authentication. Using the service allowed the mapping of wallet addresses and personal information. The figure below shows the mapping process.

Figure 28

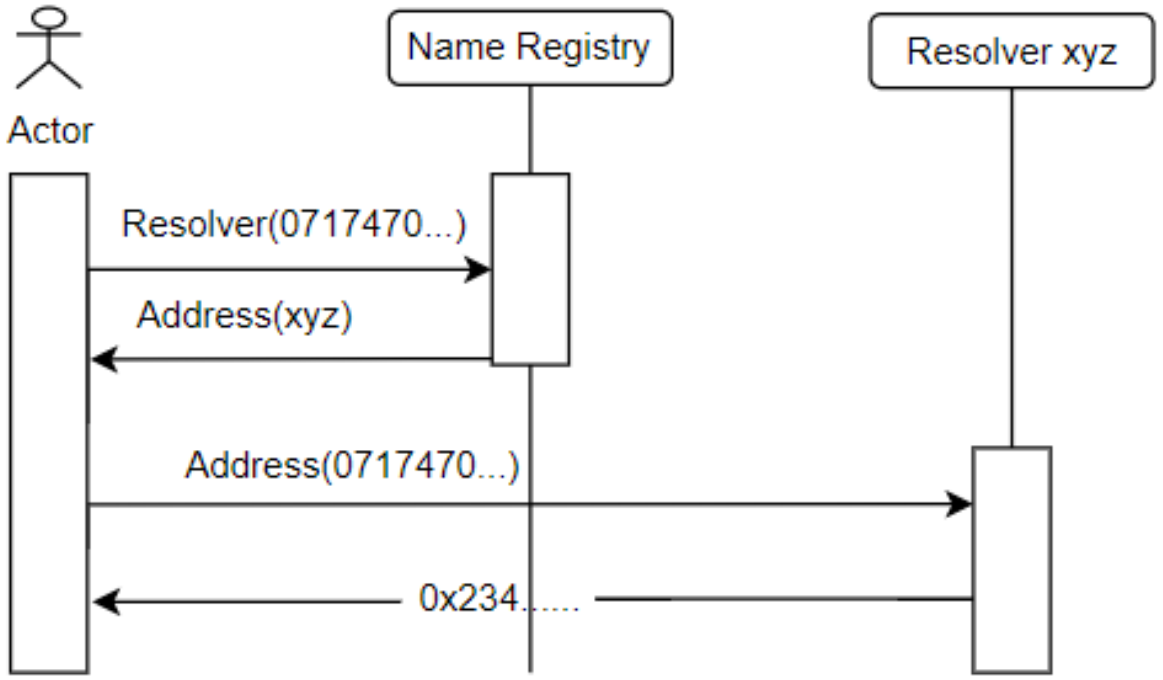
Address Mapping Process



The ENS registry consists of a smart contract that maintains a list of all domains (memorable name or identification parameter). It also stores three critical pieces of information about each domain. The owner of the domain, domain resolver, and the caching time-to-live for all records under the domain. The domain owner represents an external account (a user) and a domain registrar is a smart contract that owns a domain. The caching time-to-live however in this design is set to infinity to reduce the update overheads.

Figure 29

Address Resolution Process



Resolving a name in the name mapping system is a two-step process: The first step asks the registry what resolver is responsible for the name, and the second, asks that resolver for the answer to the query. In the example shown in the above figure, it is trying to find the blockchain address pointed to by '0717470…'. First, it asks the registry which resolver is responsible for '0717470…' Then, it queries that resolver for the address of '0717470…'.

Listing 3: User Registration Cryptographic key and address generation

```
contract ENS {
   mapping (address => string) public ens;
    mapping (uint256 => address) public phoneNumber;
```

```
 address[]  public users;
function registername( string calldata name, uint256 _No ,bytes memory signature) public {
    bytes32 meta_Hash = metaHash(name);
    address signer = getSigner(meta_Hash,signature);
   ens[signer] = name;
   phoneNumber[_No] = signer;
    users.push(signer);
 }
function getUsers() public view returns(address[] memory){
    return users;
}
function metaHash(string memory metadetails) public pure  returns(bytes32){
    return keccak256(abi.encodePacked(metadetails));
}
function getSigner(bytes32 _hash, bytes memory _signature) internal pure returns (address){
    bytes32 r;
    bytes32 s;
    uint8 v;
    if (_signature.length != 65) {
        return address(0);
    }
    assembly {
        r := mload(add(_signature, 32))
```

```
        s := mload(add(_signature, 64))
        v := byte(0, mload(add(_signature, 96)))
    }
    if (v < 27) {
        v += 27;
    }
    if (v != 27 && v != 28) {
        return address(0);
    } else {
    return ecrecover(keccak256(
        abi.encodePacked("\x19Ethereum Signed Message:\n32", _hash)
    ), v, r, s);      }   }  }
```

4.3.3 The Stable Cryptocurrency Creation

A user can create a new stable cryptocurrency by invoking the crypto conversion module. Here, a user can get cryptocurrency that is equivalent to their deposited fiat currency. This operation updates the user's wallet balance and also total market capital for the cryptocurrency.

Figure 30

The Stable Cryptocurrency Creation Process

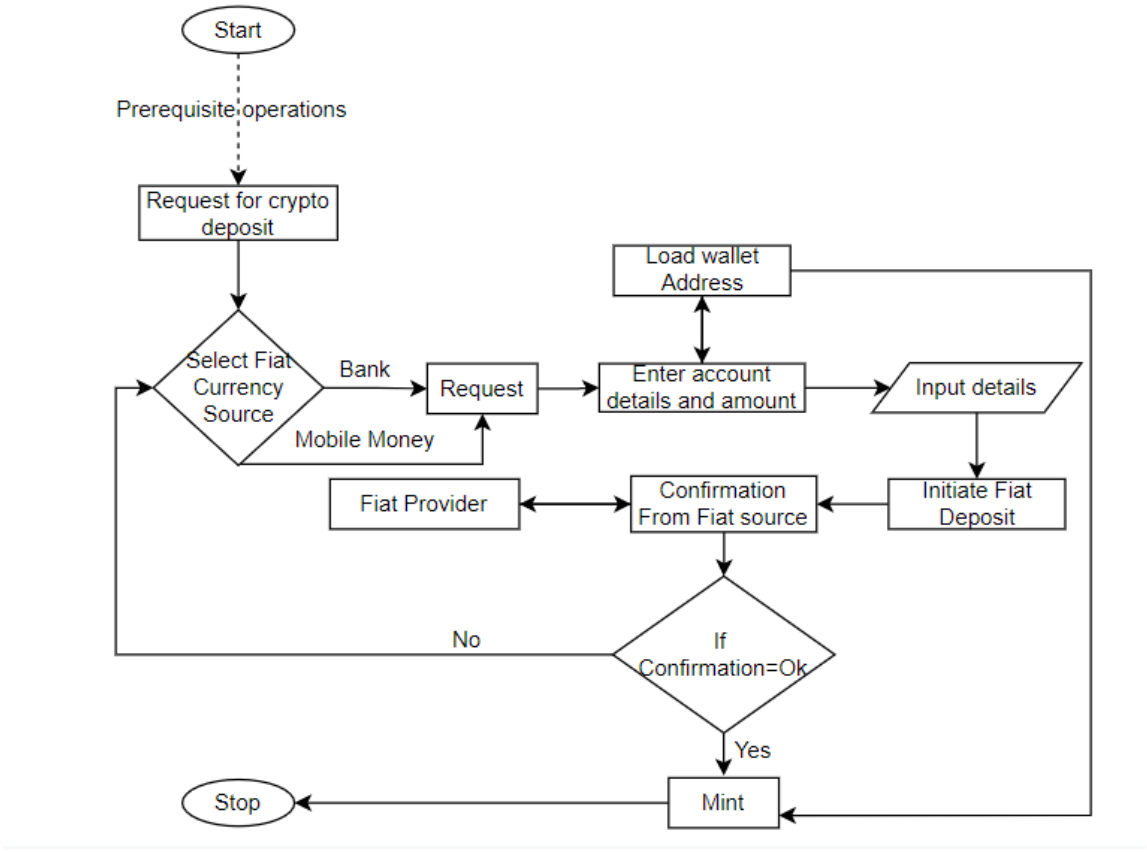
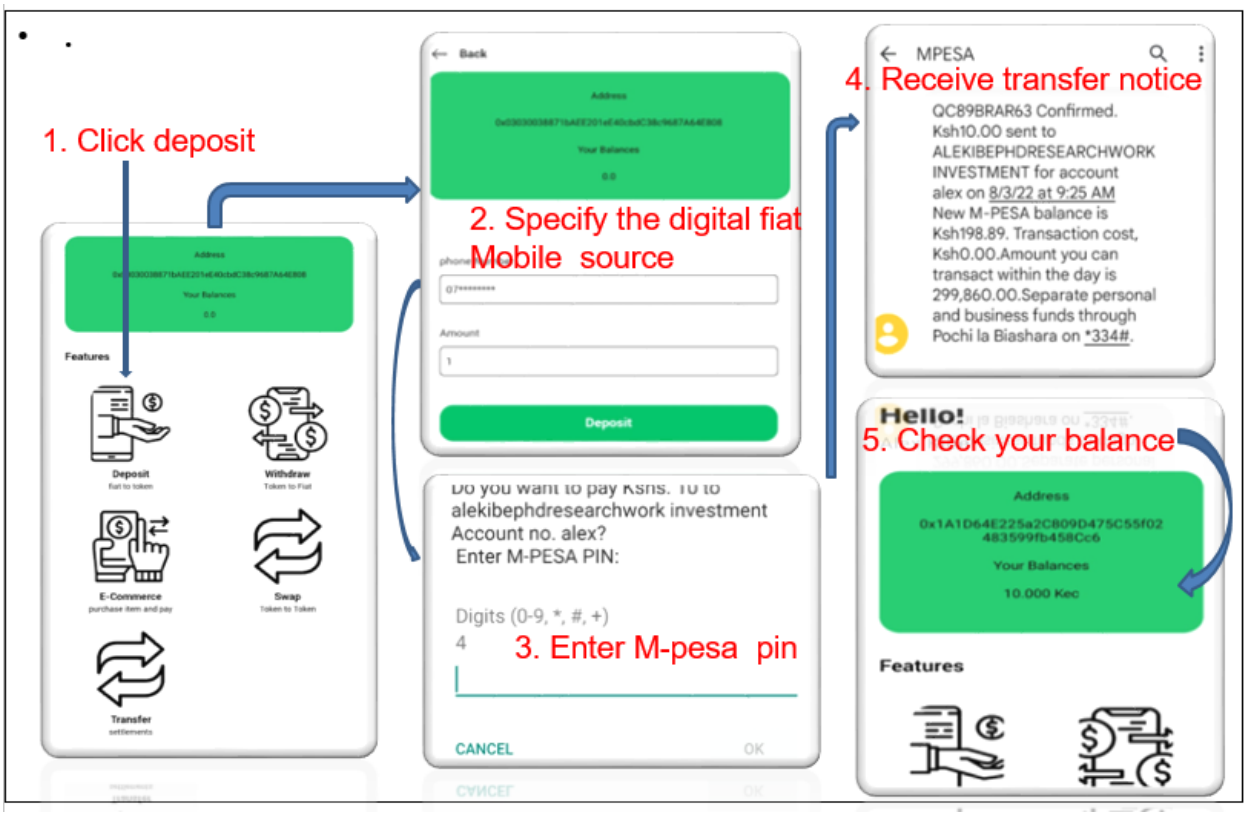


Figure 31

The Stable Cryptocurrency Creation Process



Listing 4: User Registration Cryptographic key and address generation

```
function mint(address to, uint256 amount) public virtual {
    require(hasRole(MINTER_ROLE, _msgSender()), "ERC20PresetMinterPauser: must have minter role to mint");
    _mint(to, amount);
  }
  function getSigner(bytes32 _hash, bytes memory _signature) internal pure returns (address){
    bytes32 r;
    bytes32 s;
```

```
    uint8 v;
    if (_signature.length != 65) {
        return address(0);
    }
    assembly {
        r := mload(add(_signature, 32))
        s := mload(add(_signature, 64))
        v := byte(0, mload(add(_signature, 96)))
    }
    if (v < 27) {
        v += 27;
    }
    if (v != 27 && v != 28) {
        return address(0);
    } else {
    return ecrecover(keccak256(
        abi.encodePacked("\x19Ethereum Signed Message:\n32", _hash)
    ), v, r, s);
    }
 }
}
```

4.3.3.1 The Crypto Wallet and Name

The created cryptocurrency pegs its market value to the Kenyan shilling. It achieves its price stability via collateralization (backing its values to a stable Kenya shilling). With this, the cryptocurrency wallet bore the name KENCOIN (Kenya coin). However, this did not go through the Kenyan company/ business name reservation process. Therefore, if the use of this name is legally challenged, this name may change in the future. This research considers using this name during this academic document but should this project move to full production then the legal process will be adhered to while selecting the name. Within the user account, the account balance is displayed as Kec.400.00. the following figure describes the various parts and elements within the cryptocurrency wallet

Figure 32

The Crypto Wallet and Name

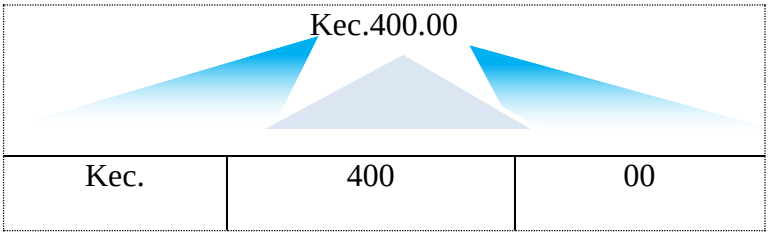


Table 9

The Crypto Wallet and Name Components

Element	Description
Kec	It Means "Kenya coin". This is to show that the underlying fiat currency is a Kenya shilling
400	The amount of cryptocurrency balance and equivalent to the peg value.
00	Cents

4.3.4 Cryptocurrency Withdrawal

Users can withdraw money from their crypto accounts. The model should be able to burn or permanently remove the cryptocurrency from circulation. The withdrawal also

Figure 33

Cryptocurrency Withdrawal

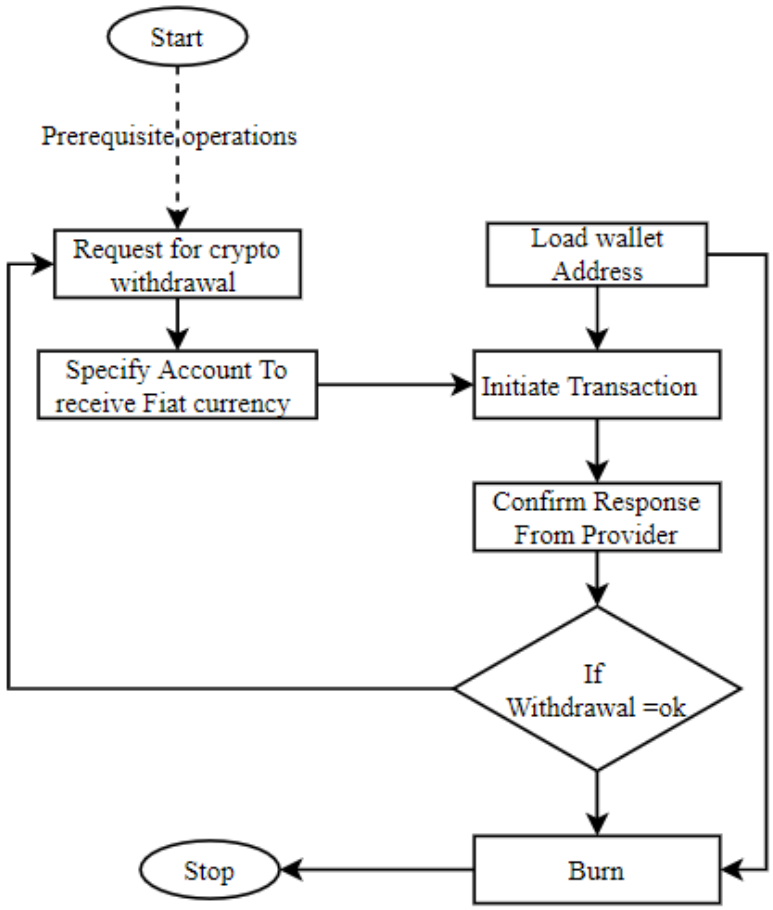
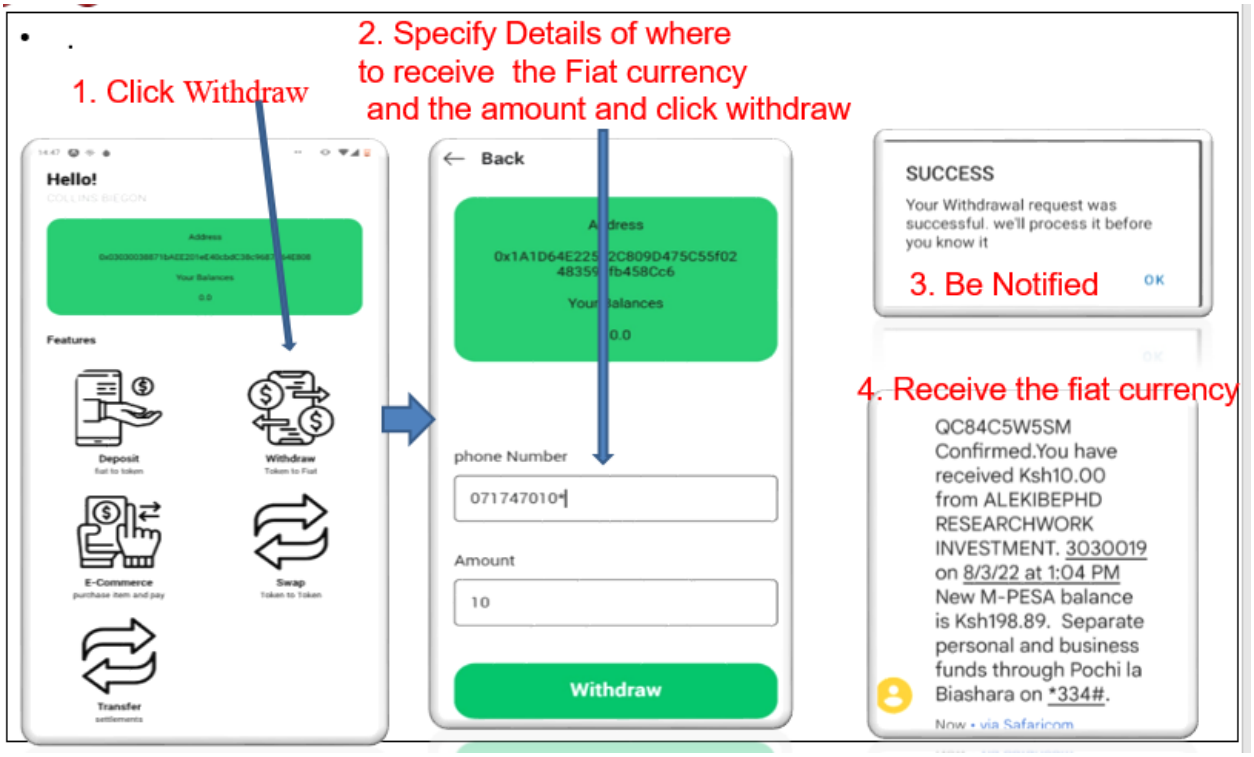


Figure 34

User Registration Cryptographic Key and Address Generation



Listing 5: User Registration Cryptographic key and address generation

```
  function burn(uint256 amount) public virtual {
    require(hasRole(MINTER_ROLE, _msgSender()), "ERC20PresetMinterPauser: must have minter role to burn");
    _burn(_msgSender(), amount);
  }
    function burnFrom(address account, uint256 amount) public virtual {
    uint256 decreasedAllowance = allowance(account, _msgSender()).sub(amount, "ERC20: burn amount exceeds allowance");
     _approve(account, _msgSender(), decreasedAllowance);
    _burn(account, amount);   }
```

4.3.5 E-commerce Platform and Send Money

Users can access e-commerce platforms and utilize their cryptocurrency. This involves paying for goods and services. This involves users who would want to send cryptocurrency from one account to another. This could be to settle debt, loan someone, or donate.

Figure 35

E-Commerce platform and Send Money

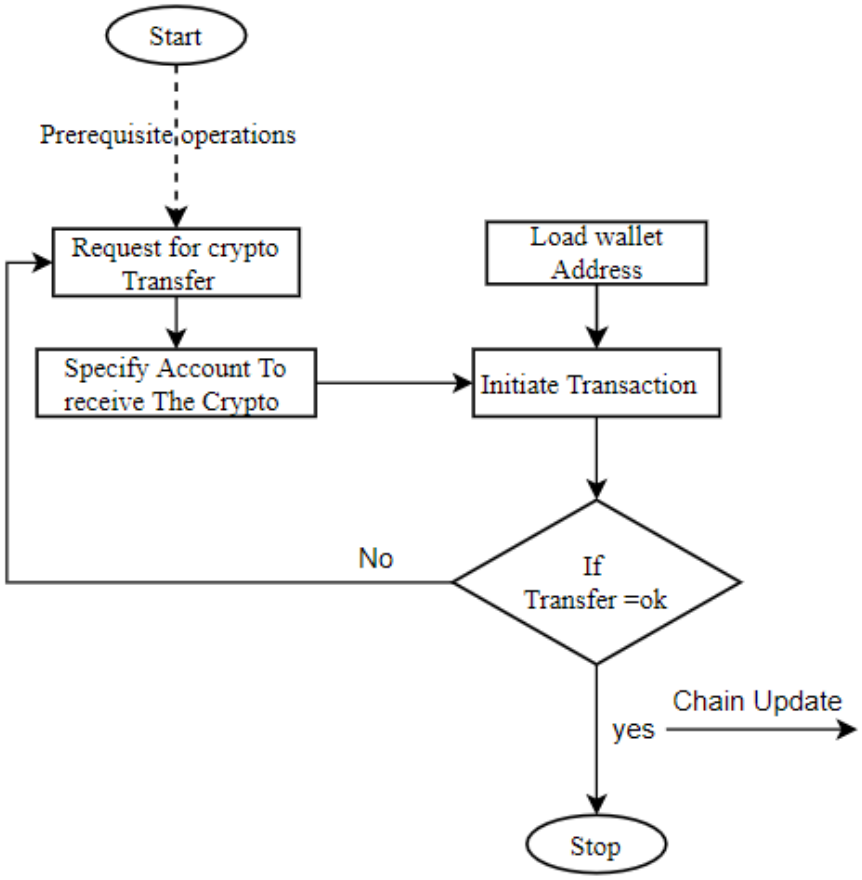


Figure 36

E-Commerce platform and Send Money

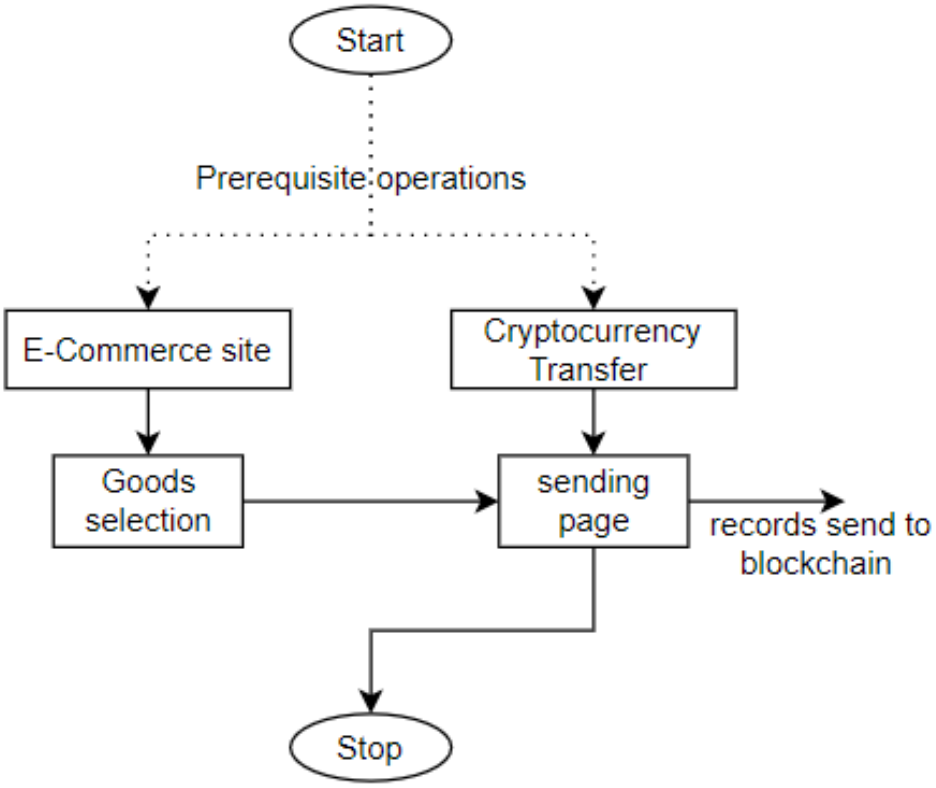
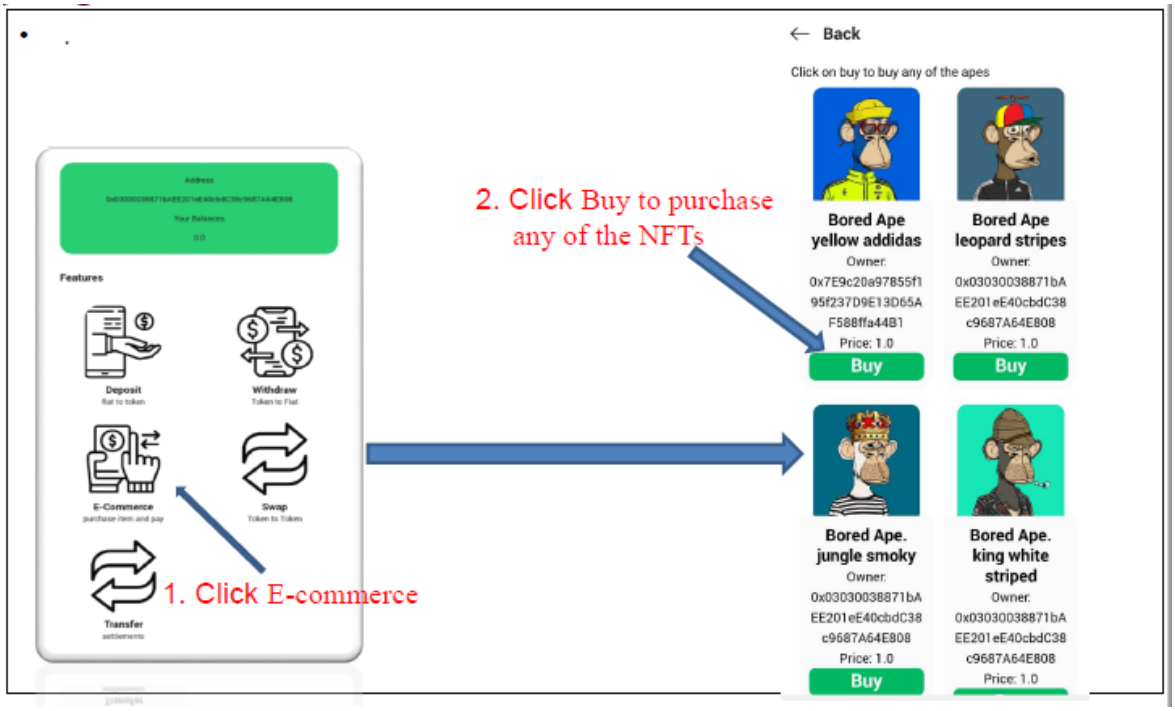


Figure 37

E-Commerce Platform and Send Money



Listing 6: User Registration Cryptographic key and address generation

```
function sellApe (uint _id,address new_owner ) public {
    BoredApe storage ape = Apes[_id];
    ape.owner = new_owner; }
```

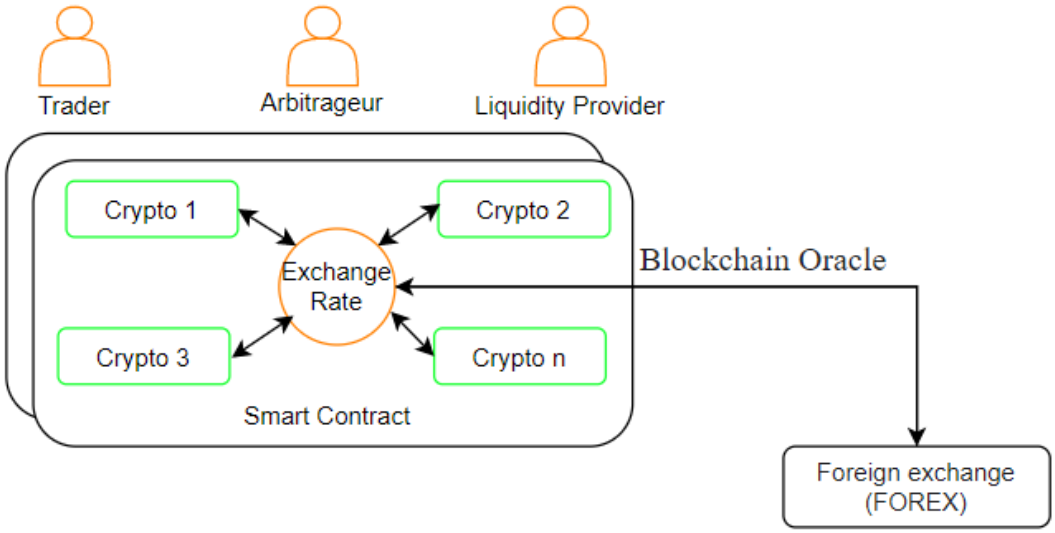
4.3.6 Converting Cryptocurrency

This module converts the cryptocurrency based on the Kenya shilling to another currency. To achieve this, a fiat-based stable currency liquidity pool is needed. The pools will housethe fiat-based stable counts in a smart contract. Within the pool, the stored cryptocurrencies can be used for exchanges, loans, and other applications. In traditional finance (Centralised Finance or CeFi), liquidity is provided by a central organization, such as a bank or a stock exchange. The pool, therefore, forms the model's exchange point. In the Liquidity pool, the liquidity providers deploy

the stable crypto assets as investments to form pools where everybody can exchange without the need for other participants. It allows crypto traders and investors to gain access to market liquidity and forms the decentralized finance (DeFi) market.

Figure 38

The Model Currency Liquidity Pool



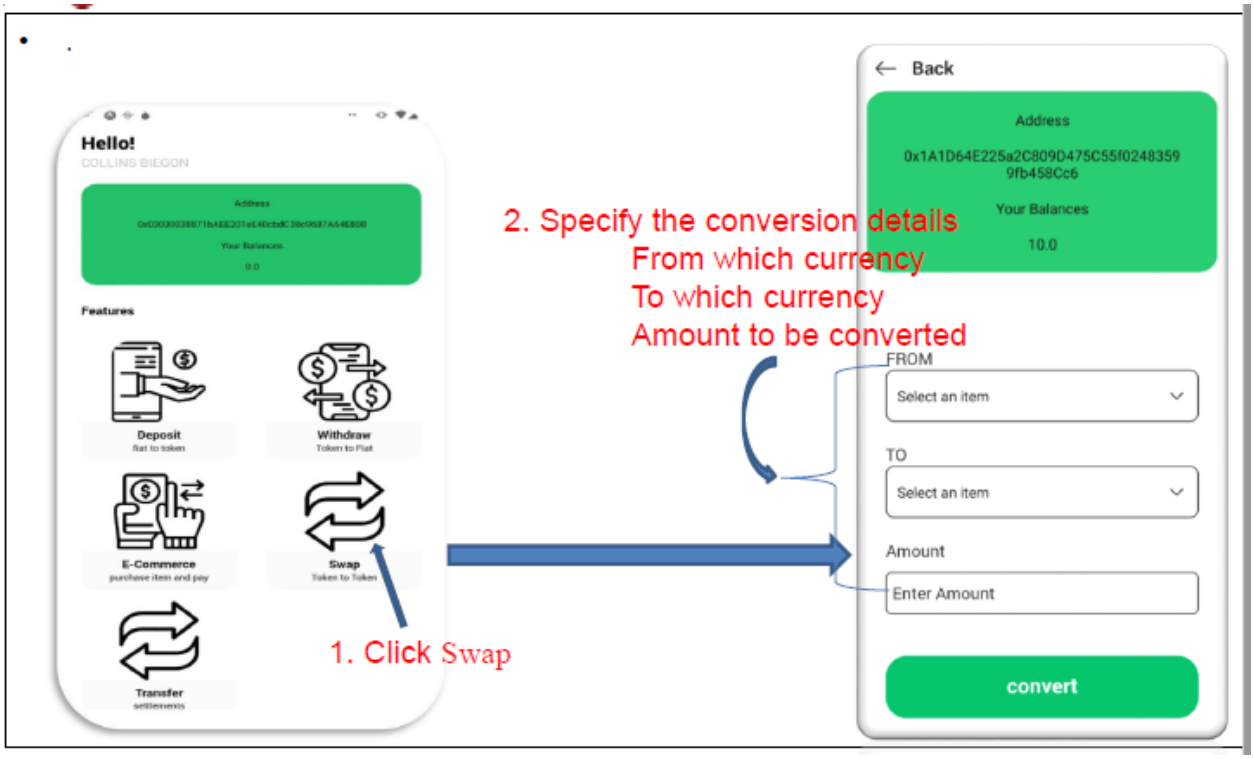
Liquidity Pool

The liquidity providers (LPs) represent individuals or professional market participants who use their stable crypto assets to provide liquidity to the liquidity pool to enable the users to access liquidity. Traders are individuals or participants that buy or sell cryptocurrencies in the liquidity pool. They are participants that require crypto exchanges. They are the ultimate clients for the liquidity pool. Arbitrageurs are individuals that enhance efficiencies in the liquidity pool. They contribute to market efficiency and serve a useful purpose by acting as intermediaries and providing liquidity. Blockchain Oracle provides a third-party service that connects pool smart contracts to the outside world, primarily to provide information from reliable real-time exchange rate sources.

Foreign exchange rates (FOREX) provide a mechanism for trading one currency for another. The real-time forex information used in this model was derived from Open Exchange Rates. This provided a simple, lightweight, and portable JSON API with live and historical foreign exchange (forex) rates for over 200 worldwide digital currencies, via a simple and easy-to-integrate API, in JSON format.

Figure 39

User Registration Cryptographic Key and Address Generation



Listing 7: User Registration Cryptographic key and address generation

```
contract Swap  {

  using SafeMath for uint256;
```

```
    mapping (address => uint256) public exchangeRates;
   event swapping (
     address user,
     string from,
     string to,
     uint256 amount   );
   function setExchange (address token , uint256 price) public  {
     exchangeRates[token] = price;
  }
   function swap ( address _tokenFrom ,address _tokenTo , uint256 amount, bytes memory signature) public {
     bytes32 meta_Hash = metaHash(_tokenFrom,_tokenTo,amount);
     address signer = getSigner(meta_Hash,signature);
    uint256 fromRate = exchangeRates[_tokenFrom];
    uint256 toRate = exchangeRates[_tokenTo];
     require(USD(_tokenFrom).transferFrom(signer ,address(this),amount));
     uint256 base  = amount.div(fromRate);
      uint256 receiveAmount = base.mul(toRate);
     USD(_tokenTo).transfer(signer,receiveAmount);
    emit swapping (signer,USD(_tokenFrom).symbol(),USD(_tokenTo).symbol(),amount);
  }
  function metaHash(address _tokenFrom ,address _tokenTo , uint256 amount) public pure  returns(bytes32){
```

```
    return keccak256(abi.encodePacked(_tokenFrom,_tokenTo,amount));
}
 function getSigner(bytes32 _hash, bytes memory _signature) internal pure returns (address){
    bytes32 r;
    bytes32 s;
    uint8 v;
    if (_signature.length != 65) {
        return address(0);
    }
    assembly {
        r := mload(add(_signature, 32))
        s := mload(add(_signature, 64))
        v := byte(0, mload(add(_signature, 96)))
    }
    if (v < 27) {
        v += 27;
    }
    if (v != 27 && v != 28) {
        return address(0);
    } else {
    return ecrecover(keccak256(
        abi.encodePacked("\x19Ethereum Signed Message:\n32", _hash)
    ), v, r, s);
```

```
    }
  }
}
```

4.3.7 Model Deployment

The model for creating stable cryptocurrency was realized using solidity for smart contracts implementation, JavaScript for building react-native for the mobile application, and Cascading style sheets version 3 (CSS3) for front-end description. It is also worth noting that various functionalities within the model were implemented by calling already existing functions, algorithms, and open libraries. The open-source development tools such as visual studio editor for editing, an expo for translation, and an android emulator. The model prototype was later deployed to a blockchain. The appropriate blockchain for deployment was selected based on the criteria presented in the following table. This intends to select a chain that could ensure that the model transactions are valid and consistent across all nodes in the distributed network.

Table 10

Chain Selection Criteria for Model Prototype Deployment

	Criteria	**Expected value (Desired feature)**
SN	**Quality description**	**Attribute (quality value)**
1.	Transaction speed/ Block time	Fast
2.	Transaction fee/ cost	Low

3.	Consensus algorithm efficiency	provide consensus for transactions and secure the chain
4.	Smart contract potential	Support powerful smart contracts
5.	Distributed application development and deployment complexity	Support simple Dapp development, another toolset compatibility, or/and with other chains
6.	API mechanism	Simple data transmission from and to a smart contract on the chain
7.	Developer community and support	Should be present
8.	Supported contract languages and presented developer experience	Should be highly available
9.	Underlying architecture complexity	Simple and easy to understand architecture
10.	Potential to integrate digital fiat currency	Allow integration
11.	On-chain, decentralized random number generator	For Block identification
12.	Chain Permissions	Permission-less
13.	Community Support	Wide-ranging
14.	Energy efficiency	Low computational power
15.	Usability with other tools	Support tools like wallets and metamask
16.	Presents of Virtual Machines	Virtual machine to host and run smart contracts

The distributed ledger technology or chain adopted for use in this study that inhabits the above requirements and satisfies the selection criteria specified above is ropsten Ethereum network. The ropsten network is also preferred since its testnet is similar to the ropsten mainnet. The Proof of Work (POW) consensus protocol used in the ropsten testnet is the same as the mainnet, and the test Ether can be mined or freely requested from ropsten faucet. It is an open-source enterprise-grade distributed ledger technology (DLT) platform, designed for use in enterprise contexts and accommodates the underlying requirements not limited to the highlighted above. In addition, the ropsten Ethereum network supports a modular architecture, which was a key design consideration for this model, and it has robust security architecture. It is configurable, versatile, optimizable, scalable, and open to innovation. With the ropsten infrastructure, the development was able to effectively support and manage the user accounts, provide transaction processing, confirmation, and record immutability.

4.4 Model Evaluation

The viability of the concept and demonstration of workability was done to ascertain the model's practical potential. Prototyping was used as a valuable exercise to allow visualization of product functioning by providing an interactive model of end product design, navigation, and layout. This section presents an evaluation of the model performance. The model evaluation checks the user Interface, APIs, Database, Security, communication, and other functionalities.

The evaluation was split into two parts. The model was tested against the functional requirements and specifications in the first phase to ensure that the model requirements and specifications were met effectively. This was a purely technical evaluation that used test cases to see if it met the model's requirements. To identify the model quality, the second phase evaluates the model using the software quality model. As stated in section 4.4.3 below, the ISO/IEC 9126 software quality

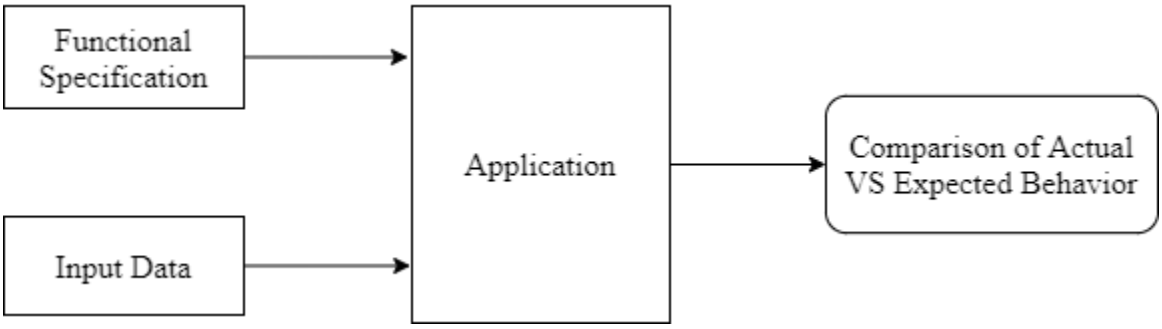
model was used to categorize software quality into six characteristics (factors) that are further subdivided into sub-characteristics (criteria). Pilot testing, which targeted the potential users, was utilized to check the model under real-time operational conditions in order to determine its quality.

4.4.1 Functional Testing

As previously stated, the goal of this methodology was to evaluate the created model against the functional requirements/specifications. Each functional requirement in the model's minimum viable product was tested by giving acceptable input and comparing the output to the functional requirements as shown below.

Figure 40

Functional Testing



The functional approach of model effectiveness was used to establish model functions first, and t hen to build criterion measures to assess how well the objectives were met. The functional requir ements of the evaluation model were then transformed into test cases. The test case specifications, steps for execution, and the expected results were defined as shown below. Each test case was run and the results were kept track of.

Table 11

The Model Test Cases to Compare the Output

TC- ID	Specifications	Steps To Execute		Expected Results	Status
TC-01	Check if the model can allow users to create profiles or accounts with the model using the user's name, phone number, and any other information necessary for KYC. (Key creation)	1	Have a potentially new user	It should save the user details and allow the user to access the model. Also, the user's data should be protected using encryption.	
		2	Generate a biodata for the user		
		3	Fill in the user information		
		4	Click on the register/submit button		
TC-02	Check if the user can access model services upon account creation.	1	Try to access it on a different phone without the model setup	It should allow the user to access the model services only after account creation and for the otherwise case, the model shouldn't allow access	
		2	Reload the mobile after successful registration in the TC-01		
		3	Check if the user accesses the model services		
TC-03	Check if a user can buy cryptocurrency based on the fiat-token operation	1	Raise a request for crypto	It should allow debiting of the user's crypto account with an equivalent fiat currency.	
		2	Permit fiat currency transfer from the selected digital account.		

		3	submit an equivalent digital fiat currency		
		4	Wait for response		
TC-04	Check if a user can liquidate his/her account (convert his crypto to fiat currency)	1	Initiate the conversion process	It should allow conversion or liquidation service of crypto to fiat currency. in the event of withdrawing more than the balance then it should display an error message.	
		2	Specify the amount of crypto to convert more than the current balance.		
		3	Repeat the same process 2 with a valid amount		
		4	Click on submit button		
TC-05	Check if a user can use his/her cryptocurrency to pay for goods and services	1	Check for goods and services to buy	It should allow a user to pay for items by crediting their accounts and showing the ownership of the item purchased	
		2	Select the item for purchase		
		3	Click on the buy button		
TC-06	Check if the stable coin can be converted into another cryptocurrency	1	Specify the user account details	The model should allow users to convert their cryptocurrencies from having Kenya shillings as the base currency to another	
		2	Specify the base currency		
		3	Then run		
TC-07		1	Access the transfer module		

	Check if the created cryptocurrency can be transferred from one account to the another	2	Initiate transfer with negative and positive data	The model should only allow the transfer of cryptocurrencies less than the current balance.	
		3	Specify the recipient's details		
		4	Then submit		
TC-08	Check if the distributed data can be accessed by the network crews	1	Open the host network	The transaction records must have been recorded in the blockchain platform. The entire blockchain-based information about the transactions must be transparent	
		2	Open the ropsten etherscan		
		3	Search the details with the user account address		

	The Test Case status definitions are	
	Passed (P):	Test run-result matches the expected result
	Failed (F):	In some cases: i) Test run-result did not match the expected result ii) The result did match as per expectation but caused another problem.
	Not Run (NR):	The test has not yet been executed either because of the module malfunction or action needed

4.4.1.1Test Status Reporting

The test cases were run and the results were kept track of. To assess whether the functionality is performing as expected, the actual result after executing the test case was compared to the expected output (derived from the requirement specification). The system test revealed that it was indeed feasible to deliver a model for creating stable cryptocurrency using fiat currency. The overall test was a pass. The test results are presented in the table below.

Table 12

Test Status Reportin

TC ID	TC-01	TC-02	TC-03	TC-04	TC-05	TC-06	TC-07	TC-08
Status	P	P	P	P	P	P	P	P
FT	A	B	C	D	E	F	E	H and G
Key • **FT-Functionality Traceability** • **P-Passed**								

4.4.2 Pilot Testing

The purpose of this study was to come up with a model for creating stable currency using fiat currency to enhance global electronic commerce. It aims to revolutionize the current financial system by establishing an inclusive and stable global virtual currency that operates on the innovative blockchain infrastructure. The objective of the proposed system is to enable users to register and create a cryptocurrency by depositing a fiat currency using a mobile money transfer (M-pesa) or a debit card (GT bank card). The deposited Fiat currencies invoke a smart contract to create an equivalent cryptocurrency and deposits to the user's cryptocurrency account. The user can use the cryptocurrency in various ways. For demonstration, this research based on the user

stories defined in the functional requirement section created four tasks that a potential user could accomplish with the model.

Firstly, a user would use cryptocurrency to pay for goods and services. To demonstrate this functionality a Non-Fungible Tokens (NFT) was added to the model for purchase. NFTs are unique cryptographic tokens that exist on a blockchain (Cornelius, 2021). They represent real-world items like artwork and real estate. The NFTs on this pilot test however do not have real-world value.

Secondly, a user could also wish to transfer cryptocurrencies to another account. This represents those informal transactions like donations, lending, payment for debts, or friendly awards. Although blockchain transfer involves sending cryptocurrencies from one address to another, this research designed a simpler way to represent a user's address using a phone number to improve the user experience.

Thirdly, a user would wish to exchange their cryptocurrency from one currency to another (example based on Kenya shilling to Uganda shilling). The model implemented a liquidity pool to accomplish this task. The pool uses blockchain oracles to read real-time currency exchange rates from a trusted source. The model used exchange rates from Open Exchange Rates.

Lastly, a user could also take off his or her cryptocurrencies out of the chain. Here, the model design assumed that in some cases a user would want to spend his or her currency on platforms that do not accept cryptocurrencies. To implement this need, withdrawal functionality was added. By withdrawing, a user gets back his or her currencies in fiat form. The model was implemented with these requirements to serve as a minimum viable product and therefore was accessed purely based on using thesefunctional features and other usability-based attributes.

The pilot testing was selected as the most effective method of evaluation because it was relatively inexpensive and would give a true picture of the research idea and the practical implementation

possibilities. A suitable google form for collecting feedback and analysis as a high response rate was expected with anonymity preserved. The pilot testing was designed to retrieve information based on the ISO 9126 Framework and validate the functional testing.

4.4.2.1 Pilot Testing Sample Selection

The pilot testing was conducted to test the above model functionalities and to explore any issues surrounding user experience. An initial target of 50 smartphone users to represent the potential was envisioned. We targeted smartphone users because they can install the model's mobile app to easily operate and access mobile money within the same phone. However, it also takes into account situations where users want money from a line operated by another phone. To be able to reach diverse individuals, the pilot testing procedures, instructions, and model were distributed through micro-works. Isaac and Michael (1995) and Hill (1998) suggested 10 – 30 participants for pilot testing. Julious (2005) also suggested 12 participants for pilot testing. Because of these suggestions, through the micro-works platform, 50 users were targeted.

4.4.2.2 Piloting Procedure

The procedure for the pilot testing based on the selected Kallio et al (2016) framework is outlined below;

The pilot testing started by preparing all the necessary tools for the pilot testing. This preparation included model deployment to the Expo platform and a link for download generated. A manual for model usage and guidelines to lead users to realize the testing objective was also prepared. In addition, an accurate description of the model and the intentions regarding the model were given. This was followed by an agreement with the micro-works agent on how he would be compensated for the service and the time limit. An ethical consideration as expected of this research and the research team was also explained to the agent and ensured that it was understood. Upon agreement

with the micro-works agent, the model, and the model testing guidelines were deployed into the microwork's platform for testing. The target participants accessed the model and guidelines and interacted with the model.

After the first 31 participants were through with the testing, their inputs about what they felt about the model and what changes would improve the model performance were shared via a google form. Every suggestion was considered and implemented. Appendix VII contains the materials utilized in the model's pilot testing.

4.4.2.3 Pilot Testing Report for Functional Testing Validation

The first pilot testing was carried out over three weeks. During this period, a total of 31 users and their transactions and feedback is presented in table 13 below.

Table 13

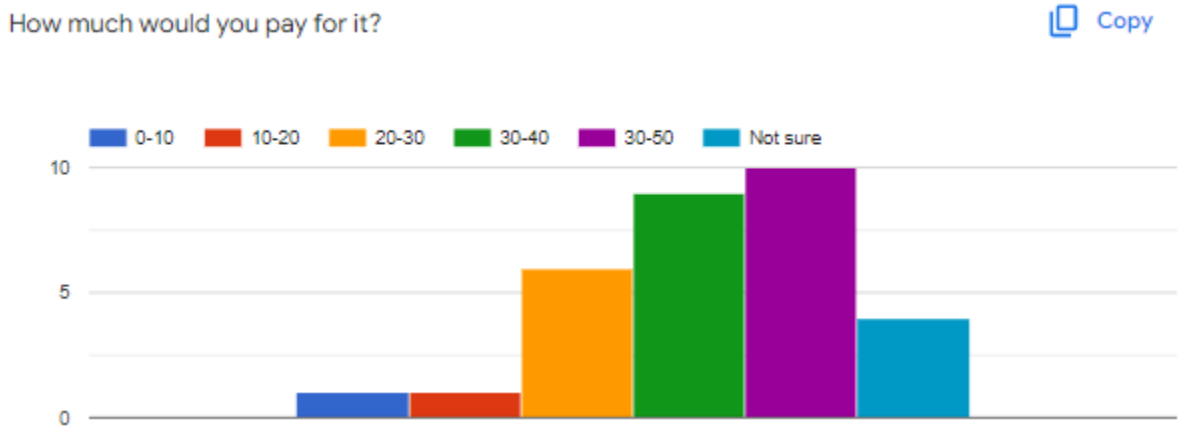
User Views on The Model Prototype

SN	Item	Responses	Yes	No
1.	I was able to create a cryptocurrency	31	87.5 %	12.5%
2.	I was able to buy NFTs artwork using my cryptocurrency	31	85 %	15 %
3.	I was able to convert my cryptocurrency from the Kenya shilling to another currency	31	72.5 %	27.5%
4.	I was able to withdraw my cryptocurrency and get my original currency	31	82.5 %	17.5%
5.	I would use the model in the event it is put into full deployment	31	75 %	25%
6.	I would pay to use this system	31	90 %	10%

Most pilot testing participants, 87.5 %, indicated that they were able to create a cryptocurrency equivalent to their deposited fiat currencies. With their cryptocurrency, the majority of the users were able to use it in various ways. 85 % were able to buy NFTs artwork used to represent eCommerce and 72.5% were also able to convert their currencies into other forms and back to Kenya shillings with the current exchange rates. At the end of the interaction, all users were able to withdraw their cryptocurrencies. A majority of them were also willing to continue using the model if it is put into full production and also agreed that the platform fee would be okay provided it is favorable to the end-user as shown below.

Figure 41

Possible Payment Fee to Use the Model



4.4.3 Model Evaluation Based on ISO 9126 Quality Model

This section presents the model evaluation based on the ISO 9126 Quality Model (ISO 1991) tool. The ISO 9126 model was developed by the International Organization for Standardization (ISO) and is one of a large group of internationally recognized standards applicable across a wide range of applications (St-Louis & Suryn, 2012). To determine the model quality, metrics to measure various model quality attributes based on the ISO guidelines were designed. Software metric is a

measure of software characteristics that are measurable or countable. It measures software performance, productivity, and many other uses for software quality improvement. For this study, the model quality evaluation was undertaken by measuring how well it conforms to the six characteristics: functionality, reliability, usability, efficiency, maintainability, and portability as stipulated in ISO 9126. The ISO 9126 is the standard and framework provided by ISO for information technology for the evaluation of software quality (Bhatti, 2005). Each characteristic is subdivided into related sub-characteristics and a statement/ declaration for evaluation. Each of this characterization is based on the feedback from the pilot testing and the expert analysis of the model during the functional testing.

i) Functionality

The functionality attribute tests whether the model satisfies the functional requirements and the overall objective of the study. As guided by ISO 9126 framework, the functionality attribute is subdivided into Suitability, Accuracy, and Security Sub-Characteristics. A statement to gauge the degree of satisfaction was created based on these Sub-Characteristics.

ii) Reliability

This attribute tests the model to establish the ability to maintain a level of performance under special conditions. The sub-attribute that guided statement generation is fault tolerance and recoverability.

iii) Usability

This set out attributes that bear on the effort needed for use by an implied set of users. The various usability attributes considered include Understandability, Learnability, Operability, and Attractiveness. These attributes were designed in the view of the users. For instance, model

understandability is defined as the capability of the model to enable the user to understand whether the model is suitable, and how it can be used for particular tasks. Theoperability measures how well the model works in a production environment, for end-users. It also involves a good user interface that utilizes the principles of a well-defined target audience, intuitive user navigation, and consistency throughout a digital product.

iv) Maintainability

The design also sets out attributes that bear on the effort needed to make specified modifications. From the design philosophies, this model intends to support future changes and simplify manageability while maintaining stability. The model also was testable through functional testing and pilot testing

v) Portability

This set out attributes that bear on the ability of the model to be transferred from one environment to another. These include Adaptability, Installability, Co-existence, and Replaceability.

vi) Efficiency

Relationship between level of performance and number of resources required/used. The sub-attributes considered for efficiency evaluation include time behavior and resource utilization.

Table 14

ISO 9126 Characteristic and Sub-Characteristics

SN	ISO 9126 Characteristic Sub-Characteristics		Declaration/ Statement
1	Functionality	Accuracy	The model was able to provide accurate results for every functionality
		Suitability	The functionalities and help tools provided were sufficient in helping me complete my interaction
		Interoperability	The model was able to run on my device without affecting the operations of other applications
		Compliance	The model has all the key functions and capabilities I expect it to have
2	Reliability	Fault Tolerance	The model functionalities are readily available for use by any registered user (The model didn't crush even when wrong data is entered)
		Maturity	The model has a good design
			The model has a verifiable operation
		Recoverability	The model can recover from errors, especially in the case of wrong data input
3	Usability	Learnability	It was simple to learn and use the model
			The information display is clear
			The use of words was nonambiguous

		Efficiency	Using this model, tasks were quickly completed
		Memorability	It was easy to get re-established to the model even after opening other modules
		Attractiveness	The model has an enjoyable interface
			The model has consistent use of colors
			I love the use of symbols and conventions in this model
		Subjective Satisfaction	I feel comfortable using this model
			I feel empowered with this model
			Overall, I am satisfied with this model's performance
4	Maintainability	Stability	The model can withstand unexpected events
		Testability	The model functionalities can effectively and efficiently be performed
		Analysability	The model can be diagnosed to identify areas for improvement
			The model can be operated and fault identified
		Changeability	The model can be modified to make it more resilient without compromising its goal
			A new feature can be added to this model

5	Portability	Adaptability	The model can adapt to future changes
			The model can accommodate new features
		Installability	I was able to download and install the model
			The model installation was successful
		Co-existence	The model was able to run on my device without affecting the operations of other applications
		Replaceability	The model components can be replaced
6	Efficiency	Time Behaviour	The model performance is time responsive and satisfying
		Resource Utilization	The model adequately utilizes all its supplied device resources to help effectively perform specified tasks

The model characteristics and sub-characteristics represent evaluation features defined based on the ISO quality model. It covers a wide spectrum of model features, including both technical specifications and human interaction with the model. For example, it includes HCI features such as the attractiveness of the interface, which is overlooked by the other quality models.

4.4.3.1 Model Quality Evaluation Methodology

The research used the ISO 9126 based quality characteristics and sub-characteristics to evaluate the model. The evaluation focused on the use of the model by potential users during pilot testing. The participants downloaded the model from https://exp-shell-app-assets.s3.us-west-1.amazonaws.com/android/%40grandmullah/KENCOIN-2400474c6b2445eaaac9dae6a7f0c61c-

signed.apk , installed and used it to accomplish various tasks. Interaction guidelines shown in appendix vii were presented to the participants to enhance the user experience.

During the investigation, several evaluation methods were employed. Firstly, the evaluation focused on the model based on the user's experience. Here, the users interacted with the model and provided their feedback via a google form available at https://forms.gle/yFtQmNaTrSvSveGv6. From the researcher's point of view, Functionality, Reliability, and Usability characteristics could easily be assessable, whereas the remaining characteristics are difficult to measure except by trained IT professionals. For this reason, the focus hereis on these characteristics. Secondly, it evaluated the model based on this quality model using blockchain expert users. Thirdly, the evaluation also used the model-generated report to ascertain that various users were able to accomplish various tasks within the model.

4.4.3.2 Quality Evaluation Results

The results were summarized into a matrix relating the characteristics and sub-characteristics to the main tools offered in table 15. The values in the metrics indicate the total users that thought that the tool satisfies the requirements of the sub-characteristic and the declaration statement.

Table 15

Summary Model Evaluation Based on ISO 9126 Metrics Framework for Software System

SN	ISO 9126 Characteristic Sub-Characteristics		Declaration/ Statement	Strongly Disagree	Disagree	Neutral	Agree	strongly Agree	Total
1	Functionality	Accuracy	The model was able to provide accurate results for every functionality	1	4	2	19	8	29
		Suitability	The functionalities and help tools provided were sufficient in helping me complete my interaction	2	3	2	10	12	29
		Interoperability	The model was able to run on my device without affecting the operations of other applications	1	3	2	11	12	29
		Compliance	The model has all key functions and capabilities I expect it to have	2	5	2	12	8	29

2	Reliability	Fault Tolerance	The model functionalities are readily available for use by any registered user (The model didn't crush even when wrong data is entered)	1	4	2	7	15	29
		Maturity	The model has a good design	2	3	3	10	11	29
			The model has a verifiable operation	1	4	4	12	8	29
		Recoverability	The model can recover from errors, especially in the case of wrong data input	1	3	5	12	8	29
3	Usability	Learnability	It was simple to learn and use the model	1	4	2	11	11	29
			The information display is clear	1	3	3	7	15	29
			The use of words was nonambiguous	0	2	6	13	8	29
		Efficiency	Using this model, tasks were quickly completed	1	2	5	10	11	29

		Memorability	It was easy to get re-established to the model even after opening other modules	1	4	4	10	10	29
		Attractiveness	The model has an enjoyable interface	1	3	3	13	9	29
			The model has consistent use of colors	1	4	2	10	12	29
			I love the use of symbols and conventions in this model	1	2	4	13	9	29
		Subjective Satisfaction	I feel comfortable using this model	1	4	3	10	11	29
			I feel empowered with this model	1	2	4	11	11	29
			Overall, I am satisfied with this model's performance	1	3	3	7	15	29
4	Maintainability (Internal Quality	Stability	The model can withstand unexpected events	0	0	0	2	2	4
		Testability	The model functionalities can effectively and efficiently be performed	0	0		3	1	4

		Analysability	The model can be diagnosed to identify areas for improvement	0	0	1	2	1	4
			The model can be operated and fault identified	0	0	1	1	2	4
		Changeability	The model can be modified to make it more resilient without compromising its goal	0	0	0	2	2	4
			A new feature can be added to this model	0	0	1	2	1	4
5	Portability (Internal Quality Attributes)	Adaptability	The model can adapt to future changes	0	0	0	1	3	4
			The model can accommodate new features	0	0	1	2	1	4
		Installability	I was able to download and install the model	0	0	1	1	2	4
			The model installation was successful	0	0	0	2	2	4

		Co-existence	The model was able to run on my device without affecting the operations of other applications	0	0	0	3	1	4
		Replaceability	The model components can be replaced	0	0	1	3	1	4
6	Efficiency	Time Behaviour	The model performance is time responsive and satisfying	1	3	5	12	8	29
		Resource Utilization	The model adequately utilizes all its supplied device resources to help effectively perform specified tasks	1	3	5	8	12	29

4.4.3.3 Discussionof Survey Results

The model quality evaluation against the ISO 9126 standard criteria provided a range of feedback on a wide range based on the six characteristics. Although the standard provided user perceptions towards the model as presented above. This research believes that out of the six standard quality characteristics only four: functionality, usability, reliability, and efficiency reflect the user's perception of the quality of a model product. Portability and maintainability do not appear to be concepts of prime concern to the operational user, except in terms of how they influence the other four characteristics. This is because the operational users are primarily concerned with "how easily, reliably, and efficiently can they use the software as-is?" Whether they can use it in another hardware or software environment and how easy it is to diagnose and rectify faults in it, is of relatively low importance unless it impacts the model's functionality, reliability, usability, or efficiency of operations. To evaluate Portability and maintainability attributes, four blockchain experts were approached to evaluate the structural properties of the model. In respect to ISO 9126 framework, this was intended to evaluate the model maintainability and portability quality attributes.

4.6 Limitations and Challenges in Implementing the Model for Creating Stable Cryptocurrency Using Fiat Currency

The model for creating stable cryptocurrency using fiat currency for global electronic commerce was developed to provide an alternative to the present payment system. It aimed at strengthening the existing payment system by serving as a key alternative means for digital transactions built on efficiency, resilience, interoperability, universality, and high-level security. During the model development and deployment, various challenges were recorded. This section presents an evaluation of the limitations and challenges of the model prototype.

An Ethereum chain in which the developed model was deployed uses a 20-byte hexadecimal address for identification. The address needed to receive funds from another party. An address is “0xb794f5ea0ba39494ce839613fffba74279579268”. This is complex and very hard to remember. To handle this challenge, this study created a mapping system to map the user address with a memorable biodata parameter. The model mapped the user’s phone number into the blockchain address.

The user's private and public keys are generated from mnemonic words. This mnemonic words/ seed phrase also plays an important role in recovering the private key in case it is lost and therefore must be kept safe. The mnemonic words however have between 12-24 words. this is hard to remember and this study used a shared preference to store them on the user’s device.

To complete a transaction in the Ethereum blockchain, a transaction fee is required. This needs that before you initiate a transaction you must have a minimum balance more than the transaction cost in your account. Since most of the present model users, especially those to facilitate model evaluation and testing do not have this knowledge. It led to a challenge since they would not successfully run a transaction without a transaction fee. To overcome this challenge, a Meta transaction was used where the model project owner is charged for the transaction. Although this solved the challenge, for now, this isn’t a permanent solution since it`s expensive for the model owner and also limited to a few transactions.

CHAPTER 5

SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.1 Introduction

This chapter gives an overview of the study based on its findings as expressed in the previous chapter. This chapter provides a summary of the findings based on the research objectives. Then, the conclusion, recommendation, and the implication for theory, practice, and policy are presented. The chapter ends by presenting suggestions on areas for further study, and a discussion of the contribution this research has made to the body of knowledge.

5.2 Summary of Findings

Distributed Ledger Technology has emerged as one of the transformational technologies of the last decade and its introduction is gathering significant pace around the world. This technology allows for highly transparent, secure, tamper-proof transactions between parties, and creates trust withinthe environment of use. Critical use cases include supply chain verification, identity management, land registry, and many more. Perhaps the most important use cases are the payments ecosystem, where DLT can ensure secure, tamper-proof, verifiable transactions in a much simpler way as settlement and payment are the same processes. As a result, the cost of payments is significantly reduced.

For this reason, many public and private entities are investigating how this technology could provide an alternative to the present payment system and help in reducing the challenges faced currently. The Central Bank of Kenya (CBK) through a paper “Discussion paper on central bank digital currency” indicated that it has been monitoring these developments and is seeking public participation in the best way to deploy a central bank digital currency.

For the case of this study, the primary concern was to develop a model for creating stable cryptocurrency using fiat currency to enhance global electronic commerce. It aims to transform the existing financial system by establishing an inclusive global virtual currency that operates on the innovative blockchain infrastructure. The overarching goal is to empower many people in emerging economies who do not have access to banking or other financial services. The new cryptocurrency will create a new ecosystem that will enable global monetary transactions in a stable digital currency with low marginal costs. This could promote financial inclusion by improving access to financial services and capital, particularly in developing countries. At the same time, it aims to enable massive efficiency gains in developed economies, resulting in additional global economic growth.

This study set out to accomplish four goals, all of which were met by the concepts summarized i n the thesis, as well as the architecture of the application and the reasoning behind it. This sectio n contains the answers to each of the questions, which are briefly summarized below.

5.2.1 Research Objective 1: To Explore the Weakness of Existing Cryptocurrency Models Used In E-Commerce.

Research Question 1: What are the weaknesses of the existing Cryptocurrency models Used in E-commerce?

With this objective/ research question, this study reviewed the various weaknesses of the present cryptocurrencies used in e-commerce. The study considered an integrative literature review to identify and review diverse secondary data sources. To enhance rigor during the review process, Whittemore and Knafl's framework for literature review was used as a review guide. This framework defines the process of conducting a research review as incorporating a problem formulation stage, a literature search stage, a data evaluation stage, a data analysis stage, and a

presentation stage. PRISMA tools, inclusion and exclusion criteria, and a critical appraisal skills program (CASP) tool were specified and used within this study to ensure the quality of reviews. These tools aimed to assess the trustworthiness, relevance, and results of published papers during a qualitative research process. It was also used for the extraction of meaningful, relevant, and reliable information that exists in literature matching with the current study.

This study examined the various flaws of today's cryptocurrencies, which are critical in providing mission-critical support in the payment ecosystem. The findings revealed that cryptocurrencies are a poor medium of exchange, store of value, or unit of account due to a variety of flaws, which has hampered their adoption. While there have been efforts to improve the technology, there are growing concerns that cryptocurrencies still have many flaws. These include, among other things, a high level of volatility, conversion limitations, limited scalability, a lack of legislation, less liquidity, no consensus valuation approach, interoperability issues, regulatory and legal quandaries, and diversity.

According to the study, distributed ledger technology should consider other types of cryptocurrencies with a mechanism to reduce volatility. This would leverage the field of business and information technology and bridge the gap between strategic implementation of information technology systems in business. This would also realize stable and universal access to financial services for the global population, as well as efficient cross-border retail online and offline payment methods. The research also identified areas where the cryptocurrency ecosystem should be enhanced to produce better cryptocurrencies. This would improve cryptocurrency's usability and ensure its use as an alternative payment system, as well as its evolution into a broader financial infrastructure for advanced financial services such as distributed ledger savings and loan products. Table 15 summarizes how current cryptocurrencies' flaws have been addressed by model.

Table 16

Summary of Weaknesses

SN	Cryptocurrency Weakness	How it was addressed in this study
1.	Highly Volatile	The volatility of the new cryptocurrency is reduced by linking it to the government or bank-issued cash reserves. While the depreciation of fiat currencies against other currencies is a distinct possibility, large currency fluctuations are less likely.
2.	Conversion issues	The model's liquidity pool forms the exchange point. In the Liquidity pool, the liquidity providers deploy the stable crypto assets as investments to form pools where everybody can exchange without the need of other participants. It allows crypto traders and investors to gain access to market liquidity and forms the decentralized finance (Defi) market.
3.	Scalability	The model design philosophy to ensure scalability addressed this issue. Accordingly, the scalability design philosophy stated that the model should be scalable and accommodate future trends and financial ecosystem needs. The model evaluation based on the ISO 9126 manageability attribute proved that the model can accommodate future changes.
4.	Lack of Legislation	The cryptocurrency linkage to the fiat currency reserves allows it to enjoy the legislation and regulations placed by the central bank.
5.	Illiquidity and trading costs	From the model, users were able to liquidate their cryptocurrency account any time they wish. From the pilot testing, over 95% of the model users were able to withdraw their cryptocurrencies to fiat currency.
6.	Custody, clearing, and settlement problems	Although Crypto custody is about holding complex cryptographic keys (which you can think of as passwords that unlock crypto wallets) and is typically handled through wallets. The model design in this research during architectural design and implementation involved a

		data layer to keep a copy of the blockchain data. This data can be retrieved if a user loss its credentials.
7.	Valuation difficulties	The value of the created cryptocurrencies will be based on the pegged fiat currency
8.	Interoperability	The model evaluation based on ISO 9126 proved that it is interoperable. The design philosophies also considered this problem.
9.	Cryptocurrencies are unpopular	According to this study, the problem will be solved gradually by addressing volatility and other difficulties associated with cryptocurrency.
10.	Regulatory and Legal Dilemmas	The cryptocurrency linkage to the fiat currency reserves allows it to enjoy the legislation and regulations placed by the central bank.
11.	Diversity	More research is needed on this
12.	Anonymity	The KYC implemented in this research is enough to reduce anonymity. I.e. the mapping, firebase database, and the records stored in the fiat reserve.
13.	The Technology Is Still Immature	This study believes that its results and contributions will help to transform the current situation (even if it is by one step).
14.	Legal Obstacles	The cryptocurrency linkage to the fiat currency reserves allows a better chance to challenge any legal obstacle.
15.	Usability	The model usability evaluation based on the ISO usability standards showed that the model's user experience was good. The changeability of the model was also proved to be possible. This leaves room for future changes regarding the usability or functionality based.
16.	Bad Imagery	This study believes that its results and contributions will help to transform the current situation. I.e., solving the existing challenges will elevate the cryptocurrency technology towards its maturity level.

17.	Data and modelling obstacles	This study believes that its results and contributions will help to transform the current situation (even if it is by one step).
18.	Mining process	More research regarding this challenge is needed. More specifically on how to ensure quality of service and enhance user experience.

5.2.1 Research Objective 2: To Design a Stabilized Cryptocurrency Model for Global Electronic Commerce.

Research Question 2: How can a model for creating a stable cryptocurrency using fiat currency be designed?

Concerning objective two, the study sought to design a model for creating a stable cryptocurrency using fiat currency. This study created design philosophies to embody the general aims of the envisioned model in order to appropriately come up with the design. The design was also in line with the Bank for International Settlements' mutual principles (do no harm, Coexistence, and Innovation and Efficiency). The study employed focus group discussions and prospective scenarios to develop the model's functional requirements. A framework to guide the application of each approach stated to contribute to the model design was also identified. For example, the frameworks developed by Glynn, Shanahan, and Duggan for creating and contacting focus group discussions, and Rosson & Carroll's framework for scenario-based design. Through technological approaches, a design based on the model requirements and guidelines given in the expert focus group discussion and the SBD process was executed.

The intended model as a system of smart contracts was built on the design premise of having different types of contracts to conduct different classes of operations to write a safe and scalable smart contract back-end. Monax presented a concept called "The Five Types Model" to categorize

the contracts. Database contracts, Controller contracts, Contract management contracts, Application logic contracts, and Utility contracts are the different types of contracts in this model. The current model design led in Bridge Contracts, Token Contracts, and Swap Contracts based on this, the model, and the PoC functional requirement. The design is restricted to two archetypical users: the administrator and the account holder. To describe the various functional requirements that users have on the model, user stories from a focused group and the scenarios derived were written and are shown in Table 6 in section 4.2.4.2. 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 Research Objective 3: To Implement the Stabilized Cryptocurrency Model For Global Electronic Commerce

Research Question 3: How can a model design for creating a stable cryptocurrency be implemented?

This research used a blockchain-based smart contract prototype to develop a cryptocurrency that is pegged to the Kenyan shilling to achieve stability. The model design established during the study's design phase guided the implementation. This included setting up the development platform and putting the design into action to create a usable model. The implementation was modular, with the final model being created by integrating the many modules that had been completed. The following modules were implemented based on the model design:

User management module- enables model users to sign up and sign in with a lot of ease. Here user interface design and implementation principles were observed to enhance the model usability.

Conversion module- that supported crypto exchange and conversion from one cryptocurrency to another. This was facilitated by swap operation, swap API, and swap contract.

Coin creation and redemption- this creates cryptocurrency and removes it from circulation against the platform reserves. This uses the bridge API and bridge contract.

Payment for goods and services-this demonstrates the e-commerce operation and is facilitated by the e-commerce application and token transfer contract.

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 4.3.7. The entire code of the developed model is presented in Appendix I.

5.2.4 Research Objective 4: To Evaluate the Model for Creating Stable Cryptocurrency Global Electronic Commerce

Research Question 4: What is the performance of the implemented model prototype?

The assessment was divided into two parts. In the first part, the model was tested against the functional requirements and specifications to ensure that the model's requirements and specifications were met. This was a strictly technical assessment that employed test cases to see whether it satisfied the model's requirements. The second phase examined the model using the software quality model to determine its quality. Pilot testing, which was aimed at future customers, was used to evaluate the model in real-world operational conditions in order to assess its quality based on the ISO/IEC 9126 software quality model.

5.3 Conclusion

The existing crypto assets solutions that were envisioned to enable cross-border and universal payment systems still have significant flaws, according to an exhaustive review of literature and present solutions. Volatility, lack of regulation, and cryptocurrency diversity are just a few of them. The premise upon which this study was based was the need to strengthen the existing payment system by serving as a key alternative means for digital transactions built on efficiency, resilience, interoperability, universality, and high-level security. The majority of countries have created payment systems that are supported by progressive policies that encourage innovation, resilience,

consumer protection, and general stability. This research intends to improve the payment system by facilitating digital economy growth and serving as a baseline for payment systems. Any payment system's stability is critical, and this study's model is based on this goal. The payment ecosystem will be more stable and resilient as a result of this. Beyond that, monetary and financial stability, as well as the drive toward a financially inclusive economy, which is a vital enabler for overall economic growth, were top priorities.

In furtherance of these achievements, this research has followed with keen interest the discussions in addition, considerations of Bank for International Settlements and central banks across the world. Their overall vision offers potential benefits, which mirror this research's overall objective of driving a more cash-less, inclusive, and digital economy. To consolidate the gains of previous policies, this research has also chosen to develop this model with prayers that it will be put into practice soon. Specifically, the drive for financial inclusion, achieving a truly cash-less society, supporting a resilient payment system, reduction in the usage of cash and the associated cost in providing it, and increased monetary policy effectiveness are prime considerations that have motivated this study.

The success of this project means inclusive access and the ability to enable low-cost and highly efficient payments for local and cross-border transactions. It means value for money and an alternative to the country's existing payment system built for resilience and innovation.

5.4 Policy Recommendations

Blockchain technology is among the most advanced and recent themes, which have attracted the attention of both researchers and organizations due to the countless advantages and benefits it provided over the existing solution. It depicts an immutable, distributed, and decentralized ledger,

which keeps the information of the various transactions. The study made various recommendations in line with the overall study objective of the study.

The primary concern of the study was to develop a model for creating stable cryptocurrency using fiat currency to enhance global electronic commerce. The study's literature survey supported the view that the present cryptocurrencies have several limitations. To be precise, this research found 18 weaknesses. This research focused on one weakness "volatility" and by extension, some other weaknesses were addressed. This research, therefore, recommends that the government through national research funds support more search on blockchain and cryptocurrency to improve the technology and its adoption.

Many countries through their central banks are investigating how new technologies in the payment ecosystem and specifically blockchain could potentially alleviate several policy problems. The Central Bank of Kenya (CBK) should also begin its journey on investigating the potential risk and opportunities of blockchain and cryptocurrencies in the payment ecosystem. It should start with extensive study, consultations, further identification of use cases, and the testing of cryptocurrencies concept in a sandbox environment. Following the completion of the preliminary work of the blockchain Association of Kenya.

REFERENCES

Acquila-Natale, E., Iglesias-Pradas, S., & Chaparro-Peláez, J. (2019). Barriers and drivers of multi-channel e-commerce: A cross-country examination. *Dirección y Organización*, 20-32.

Allen, M. (Ed.). (2017). *The SAGE encyclopedia of communication research methods*. Sage Publications.

Arlott, A., Henike, T., & Hölzle, K. (2019). Digital entrepreneurship and value beyond: why to not purely play online. In *Digital Entrepreneurship* (pp. 1-22). Springer, Cham.

Augusto, P. A., Castelo-Grande, T., Estévez, A. M., Barbosa, D., & Costa, P. M. (2017). Method to evaluate and prove-the-concept of magnetic separation and/or classification of particles. *Journal of Magnetism and Magnetic Materials*, *426*, 405-414.

Baillon, A. (2019, August). Follow the money: Bayesian Markets to aggregate expert opinions when the majority can be wrong. *In Workshop on Fintech and Machine Learning* (Vol. 5, p. 8).

Bayram, O. (2020). Importance of Blockchain use in cross-border payments and evaluation of the progress in this area. *Doğuş Üniversitesi Dergisi*, *21*(1), 171-189.

Bez, M., Fornari, G., & Vardanega, T. (2019, April). The scalability challenge of ethereum: An initial quantitative analysis. In *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)* (pp. 167-176). IEEE.

Bhatti, S. N. (2005). Why quality? iso 9126 software quality metrics (functionality) support by uml suite. *ACM SIGSOFT Software Engineering Notes*, *30*(2), 1-5.

Boddington, P. (2017). *Towards a code of ethics for artificial intelligence* (pp. 27-37). Cham: Springer.

Bouri, E., Shahzad, S. J. H., & Roubaud, D. (2019). Co-explosivity in the cryptocurrency market. *Finance Research Letters*, *29*, 178-183.

Bouri, E., Lau, C. K. M., Lucey, B., & Roubaud, D. (2019). Trading volume and the predictability of return and volatility in the cryptocurrency market. *Finance Research Letters*, *29*, 340-346.

Brown, J. V., Crampton, P. E., Finn, G. M., & Morgan, J. E. (2020). From the sticky floor to the glass ceiling and everything in between: protocol for a systematic review of barriers and facilitators to clinical academic careers and interventions to address these, with a focus on gender inequality. *Systematic reviews*, *9*(1), 1-7.

Bullmann, D., Klemm, J., & Pinna, A. (2019). In search for stability in crypto-assets: are stablecoins the solution?. *ECB Occasional Paper*, (230).

Caddy, J., Delaney, L., & Fisher, C. (2020). *Consumer Payment Behaviour in Australia: Evidence from the 2019 Consumer Payments Survey* (No. rdp2020-06). Reserve Bank of Australia.

Cedarbaum, J. M. (2018). Elephants, Parkinson's Disease, and Proof-of-Concept Clinical Trials. *Movement Disorders*, *33*(5), 697-700.

Chen, J. (2019). Fiat money. Investopedia. Viitattu, 9, 2020.

Chohan, U. W. (2018). Cryptocurrencies as asset-backed instruments: The Venezuelan Petro. *Available at SSRN 3119606*.

Chung, L., Nixon, B. A., Yu, E., & Mylopoulos, J. (2012). *Non-functional requirements in software engineering* (Vol. 5). Springer Science & Business Media.

cnbcafrica. (2020, september 22). *Kenya ranked among world's top 10 countries in cyptocurrency adoption*. Retrieved september 27, 2020, from cnbcafrica: https://www.cnbcafrica.com/videos/2020/09/22/kenya-ranked-among-worlds-top-10-countries-in-cyptocurrency-adoption/

CoinMarketCap. (2021, 2 25). *CoinMarketCap*. Retrieved from Today's Cryptocurrency Prices by Market Cap: https://coinmarketcap.com/

Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis*, *62*, 182-199.

Cornelius, K. (2021). Betraying Blockchain: Accountability, Transparency and Document Standards for Non-Fungible Tokens (NFTs). *Information*, *12*(9), 358.

CryptoGuru. (2019, february 4). *Introducing SunGroowMall – A Nigerian Decentralized Online Store Using Crypto Coming to Kenya*. Retrieved september 27, 2020, from BitcoinKE: https://bitcoinke.io/2019/02/introducing-sungroowmall-a-nigerian-decentralized-online-store-using-crypto-coming-to-kenya/

Danielkenz. (2020). Bitcoin Ecosystem Flourishes In Kenya Despite Regulatory Constraints Around Crypto Assets. Coinnewsextra.com

Dennis, R., & Disso, J. P. (2019). An analysis into the scalability of bitcoin and ethereum. In *Third International Congress on Information and Communication Technology* (pp. 619-627). Springer, Singapore.

Dell'Erba, M. (2019). Stablecoins in Cryptoeconomics. From Initial Coin Offerings (ICOs) to Central Bank Digital Currencies (CBDCs). *New York University Journal of Legislation and Public Policy, Forthcoming.*

Dellinger, M. J., Olson, J., Clark, R., Pingatore, N., & Ripley, M. P. (2018). Development and pilot testing of a model to translate risk assessment data for Great Lakes Native American communities using mobile technology. *Human and Ecological Risk Assessment: An International Journal*, *24*(1), 242-255.

Ding, M., Soderberg, L., Jung, J. H., & Dahm, P. (2020). Low Methodological Quality of Systematic Reviews Published in the Urological Literature (2016-2018). *Urology*, *138*, 5-10.

Dong, Y. A. N. G., & Zheli, C. H. E. N. (2020). Research on the Positioning and Characteristics of Fiat Digital Currency. *Journal of Renmin University of China*, *34*(3), 108.

Eriksson, P., & Kovalainen, A. (2015). *Qualitative methods in business research: A practical guide to social research*. Sage.

European Central Bank. (2020, 9 22). *European Central Bank*. Retrieved from European Central Bank: https://www.ecb.europa.eu/home/html/index.en.html

FAUZI, M. A., PAIMAN, N., & OTHMAN, Z. (2020). Bitcoin and cryptocurrency: Challenges, opportunities and future works. *The Journal of Asian Finance, Economics, and Business*, *7*(8), 695-704.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689-707.

Gaži, P., Kiayias, A., & Zindros, D. (2019, May). Proof-of-stake sidechains. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 139-156). IEEE.

Glynn, P., Shanahan, M., & Duggan, D. (2015). Focus groups. *Available form: https://www. slideshare. net/johnglynn940/focus-groups-presentation [Diakses: 01 Mei 2020]*.

Gordon, N. (2017). Flexible pedagogies: Technology-enhanced learning. From the report series Flexible Pedagogies: Preparing for the Future. The Higher Education Academy, January. Online at: http://www.heacademy.ac.uk/resources/detail/flexiblelearning/flexiblepedagogies/tech_enhanced_learning/main_report (accessed 20 December 2020).

Hanington, B., & Martin, B. (2019). *Universal methods of design expanded and revised: 125 Ways to research complex problems, develop innovative ideas, and design effective solutions*. Rockport publishers.

Hansson, M., & Manfredsson, A. (2020). "We Traded Our Privacy for Comfortability": A Study About How Big Data is Used and Abused by Major International Companies.

Helo, P., & Hao, Y. (2019). Blockchains in operations and supply chains: A model and reference implementation. *Computers & Industrial Engineering*, *136*, 242-251.

Henderson, M. T., & Raskin, M. (2019). A regulatory classification of digital assets: toward an operational Howey test for cryptocurrencies, ICOs, and other digital assets. *Colum. Bus. L. Rev.*, 443.

Hill, R. (1998). What sample size is "enough" in internet survey research? Interpersonal Computing and Technology: An Electronic Journal for the 21st Century, 6(3-4).

Hossain, R., Sarker, D., Meem, S. S., Shahrina, K., & Al-Amin, M. (2020). Analysis of Centralized Payment Eco-System: A Systematic Review on E-Payments.

Huang, Y., Wang, H., Wu, L., Tyson, G., Luo, X., Zhang, R., ... & Jiang, X. (2020). Characterizing eosio blockchain. *arXiv preprint arXiv:2002.05369*.

Isaac, S., & Michael, W. B. (1995). Handbook in research and evaluation. San Diego, CA: Educational and Industrial Testing Services.

ITU-T A.7 (2016) Telecommunication Standardization Sector Of ITU. *Focus groups: Establishment and working procedures.* Recommendation ITU-T A.7

Jalan, A., Matkovskyy, R., & Yarovaya, L. (2021). 'Shiny'Crypto Assets: A Systemic Look at Gold-Backed Cryptocurrencies during the COVID-19 Pandemic. *Available at SSRN 3796837*.

Jayatilleke, S., & Lai, R. (2018). A systematic review of requirements change management. *Information and Software Technology*, *93*, 163-185.

Jeon, S., Khoja, H., & Stita, H. (2020). Payment methods influencing purchase behavior in the clothing e-commerce: A study of millennials in Jönköping, Sweden.

Julious, S. A. (2005). Sample size of 12 per group rule of thumb for a pilot study. Pharmaceutical Statistics, 4, 287-291.

Kaal, W. A. (2020). Decentralized Autonomous Organizations–Internal Governance and External Legal Design. *Available at SSRN 3652481*.

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, *72*(12), 2954-2965.

Kang, H. J., Lee, S. G., & Park, S. Y. (2021). Information Efficiency in the Cryptocurrency Market: The Efficient-Market Hypothesis. *Journal of Computer Information Systems*, 1-10.

Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2020). Trade-offs between distributed ledger technology characteristics. *ACM Computing Surveys (CSUR)*, *53*(2), 1-37.

Katsiampa, P. (2019). An empirical investigation of volatility dynamics in the cryptocurrency market. *Research in International Business and Finance*, *50*, 322-335.

Kaur, G., & Gandhi, C. (2020). Scalability in blockchain: Challenges and solutions. In *Handbook of Research on Blockchain Technology* (pp. 373-406). Academic Press.

Kesebi, O. (2019). Disruption Ready: Building market resilience through 'adapted foresight', organizational agility, co-creative intelligence and employee engagement.

Khanom, N., & Miah, S. J. (2020). On-Cloud Motherhood Clinic: A Healthcare Management Solution for Rural Communities in Developing Countries. *Pacific Asia Journal of the Association for Information Systems*, *12*(1), 3.

Kondo, M., Oliva, G. A., Jiang, Z. M. J., Hassan, A. E., & Mizuno, O. (2020). Code cloning in smart contracts: a case study on verified contracts from the Ethereum blockchain platform. *Empirical Software Engineering*, *25*(6), 4617-4675.

Kong, X. T., Zhong, R. Y., Zhao, Z., Shao, S., Li, M., Lin, P., ... & Huang, G. Q. (2020). Cyber physical ecommerce logistics system: An implementation case in Hong Kong. *Computers & Industrial Engineering*, *139*, 106170.

Krueger, R. A., & Casey, M. A. (2002). Designing and conducting focus group interviews.

Kumar, A. (2019). Consumer perception towards e-commerce in India. *ZENITH International Journal of Multidisciplinary Research*, *9*(4), 120-128.

Lacity, M. C. (2020). Crypto and Blockchain Fundamentals. *Arkansas Law Review*, *73*(2), 363.

Lahmiri, S., Bekiros, S., & Salvi, A. (2018). Long-range memory, distributional variation and randomness of bitcoin volatility. *Chaos, Solitons & Fractals*, *107*, 43-48.

Lee, D. K. C., & Teo, E. G. (2020). The New Money: The utility of Cryptocurrencies and the need for a New Monetary Policy. Available at SSRN.

Lee, S. M., & Lee, D. (2020). "Untact": a new customer service strategy in the digital age. *Service Business*, *14*(1), 1-22.

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.

Long, H. A., French, D. P., & Brooks, J. M. (2020). Optimising the value of the critical appraisal skills programme (CASP) tool for quality appraisal in qualitative evidence synthesis. *Research Methods in Medicine & Health Sciences*, *1*(1), 31-42.

Manzoor, D., & Norouzi, A. (2020). Upstream Oil and Gas Project Financing using Oil-Backed Cryptocurrency. *Iranian Journal of Energy*, *23*(2), 7-45.

McCarthy, B., Trace, A., O'Donovan, M., Brady-Nevin, C., Murphy, M., O'Shea, M., & O'Regan, P. (2018). Nursing and midwifery students' stress and coping during their undergraduate education programmes: An integrative review. *Nurse education today*, *61*, 197-209.

Meegan, A., Corbet, S., Larkin, C., & Lucey, B. (2021). Does cryptocurrency pricing response to regulatory intervention depend on underlying blockchain architecture?. *Journal of International Financial Markets, Institutions and Money*, *70*, 101280.

Mendie, P. J., & Eyo, E. (2016). Environmental Challenges And Axiology: Towards A Complementary Studies In Eco-Philosophy. *Journal of Integrative Humanism*, *7*(1), 144-150.

Menold, J., Jablokow, K., & Simpson, T. (2017). Prototype for X (PFX): A holistic framework for structuring prototyping methods to support engineering design. *Design Studies*, *50*, 70-112.

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, *62*(1), 35-45.

Mnif, E., & Jarboui, A. (2021). Resilience of Islamic cryptocurrency markets to Covid-19 shocks and the Federal Reserve policy. *Asian Journal of Accounting Research*.

Möser, M., & Böhme, R. (2017). The price of anonymity: empirical evidence from a market for Bitcoin anonymization. *Journal of Cybersecurity*, *3*(2), 127-135.

Moin, A., Sekniqi, K., & Sirer, E. G. (2020). SoK: A classification framework for stablecoin designs. In Financial Cryptography.

monax. (2017, 12 16). the five type model. Retrieved from solidity explainer:https://monax.io/learn/smart_contracts/.

Moratis, G. (2021). Quantifying the spillover effect in the cryptocurrency market. *Finance Research Letters*, *38*, 101534.

Natea Sima, B., & Kaliyaperumal, D. (2020). The Impact of Online Social Media Networking on Educational Performance in Ambo University. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, *11*(3), 162-184.

Ndubisi, J. E. (2015). The role of philosophy in contemporary society: The Nigerian experience. *Humanity & Social Sciences Journal*, *10*(1), 40-46.

Ngunjiri, J. (2018, April 4). *Kenya: British Blockchain Bank Set to Open Office in Nairobi*. Retrieved sebtember 27, 2020, from ALLAFRICA: https://allafrica.com/stories/201804040039.html

Nikpay, F., Ahmad, R., & Kia, C. Y. (2017). A hybrid method for evaluating enterprise architecture implementation. *Evaluation and program planning*, *60*, 1-16.

O. Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). The use of focus group discussion methodology: Insights from two decades of application in conservation. *Methods in Ecology and evolution*, *9*(1), 20-32.

O'leary, D., D'agostino, V., Re, S. R., Burney, J., & Hoffman, A. (2019). *U.S. Patent No. 10,185,936*. Washington, DC: U.S. Patent and Trademark Office.

Oliveira, T. C., Gakidou, E., Vos, T., Higashi, H., & Murray, C. (2019). A systematic approach to produce robust, comparable and timely cost-effectiveness estimates for a set of interventions: proof of concept in two low-income countries. Annals of Global Health, 1(81), 64-65.

Olenina, E., & Zipunnikova, E. (2017). THE DEVELOPMENT OF CONTACTLESS MOBILE PAYMENT IN RUSSIA. In *Неделя науки СПбПУ* (pp. 353-56).

Olkhov, V. (2020). Volatility Depend on Market Trades and Macro Theory. *Available at SSRN 3674432*.

Omar, D. (2018, February). Focus group discussion in built environment qualitative research practice. In *IOP Conference Series: Earth and Environmental Science* (Vol. 117, No. 1, p. 012050). IOP Publishing.

Pandya, S., Mittapalli, M., Gulla, S. V. T., & Landau, O. (2019). Cryptocurrency: Adoption efforts and security challenges in different countries. *HOLISTICA–Journal of Business and Public Administration*, *10*(2), 167-186.

Pazarbasioglu, C., Mora, A. G., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital financial services. *World Bank Group*.

Qasim, A., & Kharbat, F. F. (2019). Blockchain technology, business data analytics, and artificial intelligence: Use in the accounting profession and ideas for inclusion into the accounting curriculum. *Journal of Emerging Technologies in Accounting*, 0000-0000.

Qureshi, S., Aftab, M., Bouri, E., & Saeed, T. (2020). Dynamic interdependence of cryptocurrency markets: An analysis across time and frequency. *Physica A: Statistical Mechanics and its Applications*, *559*, 125077.

Raj, A., Jain, N., & Chauhan, S. S. (2020). Digital Payments and its Security. *CYBERNOMICS*, *2*(2), 13-20.

Ramiz, R. (2016). New perspective for the philosophy: Re-construction & definition of the new branches of philosophy. *Philosophy*, *6*(6), 305-336.

Reed, H. (2017). Proving the proof of concept; developing new methods and knowledge to evaluate products supporting cancer therapy. *Design for Health*, *1*(1), 105-114.

Ridzuan, A. R., Ridzuan, A. R., & Ridzuan, M. (2018). Research methods in communication research. *e-Journal of Media and Society (e-JOMS)*, *1*.

Rosson, M. B., & Carroll, J. M. (2009). Scenario based design. *Human-computer interaction. boca raton, FL*, 145-162.

Sanyala, S., & Hisamb, M. W. (2019, November). Factors Affecting Customer Satisfaction with Ecommerce Websites-An Omani Perspective. In *2019 International Conference on Digitization (ICD)* (pp. 232-236). IEEE.

Schär, F. (2020). Decentralized Finance: On Blockchain-and Smart Contract-based Financial Markets. *Available at SSRN 3571335*.

Schizas, E., McKain, G., Zhang, B. Z., Garvey, K., Ganbold, A., Hussain, H., ... & Yerolemou, N. (2019). The Global RegTech Industry Benchmark Report. *Available at SSRN 3560811*.

Scupola, A., Fuglsang, L., Gallouj, F., & Vorre Hansen, A. (2021). Understandings of Social Innovation within the Danish Public Sector: A Literature Review. *Administrative Sciences*, *11*(2), 49.

Shas, H. (2108, 2 17). *SIMFORM*. Retrieved from Functional Testing: https://www.simform.com/blog/functional-testing/

Sharma, G. D., Jain, M., Mahendru, M., Bansal, S., & Kumar, G. (2019). Emergence of Bitcoin as an investment alternative: A systematic review and research agenda. *International Journal of Business and Information*, *14*(1), 47-84.

Smith, C., & Kumar, A. (2018). Crypto-Currencies–An introduction to not-so-funny moneys. *Journal of Economic Surveys*, *32*(5), 1531-1559.

Sitienei, L. C. (2020). *An Assessment of the challenges affecting electricity transmission network expansion in Kenya; a case study of KETRACO* (Doctoral dissertation, Strathmore University).

Solarin, S. A., Gil-Alana, L. A., & Lafuente, C. (2020). An investigation of long range reliance on shale oil and shale gas production in the US market. *Energy*, *195*, 116933.

St-Louis, D., & Suryn, W. (2012, October). Enhancing ISO/IEC 25021 quality measure elements for wider application within ISO 25000 series. In *IECON 2012-38th Annual Conference on IEEE Industrial Electronics Society* (pp. 3120-3125). IEEE.

Statista. (2020, 12 3). *PayPal's total payment volume from 1st quarter 2014 to 3rd quarter 2020* . Retrieved 2 8, 2021, from statista: https://www.statista.com/statistics/277841/paypals-total-payment-volume/

statista. (2020, 11 30). *Bitcoin price from October 2013 to November 27, 2020*. Retrieved 11 30, 2020, from statista: https://www.statista.com/statistics/326707/bitcoin-price-index/

Teker, D., Teker, S., & Ozyesil, M. (2020). Macroeconomic Determinants of Cryptocurrency Volatility: Time Series Analysis. *Journal of Business & Economic Policy*, *7*(1), 65-71.

Templier, Mathieu and Paré, Guy (2015) "A Framework for Guiding and Evaluating Literature Reviews," *Communications of the Association for Information Systems*: Vol. 37, Article 6. Available at: http://aisel.aisnet.org/cais/vol37/iss1/6

The Central Bank of kenya. (2022, 1 21). *Monetary Policy*. Retrieved from The Central Bank of kenya : https://www.centralbank.go.ke/monetary-policy/#:~:text=Overview,value%20of%20the%20Kenya%20shilling.

TradingView. (2021, 5 15). *Crypto market cap charts*. Retrieved from CRYPTOCURRENCY MARKET: https://www.tradingview.com/markets/cryptocurrencies/prices-all/

Tripathi, N., Oivo, M., Liukkunen, K., & Markkula, J. (2019). Startup ecosystem effect on minimum viable product development in software startups. *Information and Software Technology*, *114*, 77-91.

Umar, Z., & Gubareva, M. (2020). A time–frequency analysis of the impact of the Covid-19 induced panic on the volatility of currency and cryptocurrency markets. *Journal of Behavioral and Experimental Finance*, *28*, 100404.

U.S federal reserves. (2020, 9 22). *U.S federal reserves*. Retrieved from U.S federal reserves: https://www.federalreserve.gov/data/intlsumm/currnt.html

Valdeolmillos, D., Mezquita, Y., González-Briones, A., Prieto, J., & Corchado, J. M. (2019, June). Blockchain technology: a review of the current challenges of cryptocurrency. In *International Congress on Blockchain and Applications* (pp. 153-160). Springer, Cham.

Van Eeuwijk, P., & Angehrn, Z. (2017). How to… Conduct a Focus Group Discussion (FGD). Methodological Manual.

Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013a. URL ttps://github.com/ethereum/wiki/wik i/White-Paper.

Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International workshop on open problems in network security* (pp. 112-125). Springer, Cham.

Walther, T., Klein, T., & Bouri, E. (2019). Exogenous drivers of Bitcoin and Cryptocurrency volatility–A mixed data sampling approach to forecasting. *Journal of International Financial Markets, Institutions and Money*, *63*, 101133.

Whittemore, R., & Knafl, K. (2005). The integrative review: updated methodology. *Journal of advanced nursing*, *52*(5), 546-553.

Wischnewski, C. (2020). The Disruptive Potential of FinTechs in the German Consumer Finance Sector--A Blue Ocean Scenario?. *arXiv preprint arXiv:2007.03603*.

Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications* (pp. 1-307). Heidelberg: Springer.

Yanyan, W. (2018). Empirical Analysis of Factors Influencing Consumers' Satisfaction in Online Shopping Agricultural Products in China. *Journal of Electronic Commerce in Organizations (JECO)*, *16*(3), 64-77.

Yen, K. C., & Cheng, H. P. (2021). Economic policy uncertainty and cryptocurrency volatility. *Finance Research Letters*, *38*, 101428.

Yi, S., Xu, Z., & Wang, G. J. (2018). Volatility connectedness in the cryptocurrency market: Is Bitcoin a dominant cryptocurrency?. *International Review of Financial Analysis*, *60*, 98-114.

Yin, L., Nie, J., & Han, L. (2021). Understanding cryptocurrency volatility: The role of oil market shocks. *International Review of Economics & Finance*, *72*, 233-253.

Yin, Y., Lv, D., Huang, X., Liu, J., Xie, S., & Zhang, Y. (2021, December). Research on Blockchain Security Protection. In *2021 7th International Conference on Computer and Communications (ICCC)* (pp. 1545-1550). IEEE.

Zheng, K., Zhang, Z., & Song, B. (2020). E-commerce logistics distribution mode in big-data context: A case analysis of JD. COM. *Industrial Marketing Management*, *86*, 154-162.

APPENDICES

APPENDIX I: Informed Consent Form

KABARAK UNIVERSITY

INFORMED CONSENT TO PARTICIPATE IN A RESEARCH STUDY

This Informed Consent Form is for study participants who we are inviting to participate in a research entitled **'A Model for Creating Stable Cryptocurrency Using Fiat Currency for Global Electronic Commerce'**

1. Alex Kibet

   alexkibet@kabarak.ac.ke

   0717470102

2. Prof. Simon Karume

   skarume@kabarak.ac.ke

   0722499397

3. Dr. Nelson Masese

   NMasese@kabarak.ac.ke

   0727171725

THIS INFORMED CONSENT FORM HAS TWO PARTS:

1. **Information Sheet (to share information about the research with you)**
2. **Certificate of Consent (for signatures if you agree to take part)**

You will be given a copy of the full Informed Consent Form

PART I: INFORMATION SHEET

Introduction

I am Alex Kibet, a PhD in Information Technology candidate at Kabarak University. We are doing research on creation of stable cryptocurrency using fiat currency for global electronic commerce. The purpose of your participation in this research is to help the researcher in defining possible model functional and non-functional requirements. You were selected as a possible participant in this study because of your experience in blockchain application development. Before you decide, you can talk to anyone you feel comfortable with about the research.

Purpose of the research

Cryptocurrency technology and crypto tokens were originally envisioned to provide universal access to financial services for a large share of the world's population and efficient cross-border retail payments. Research has however shown that cryptocurrency prices are highly volatile, responding strongly to global events and speculative concerns about the cryptocurrency market. This research involves the creation of a model that would create a stable cryptocurrency that pegs its value on a fiat currency thus reducing volatility. This would leverage the field of business and information technology to bridge the gap of strategic implementation of information technology systems in business to realize stable and universal access to financial services for the larger world's population and efficient cross-border retail online and offline payments methods.

Type of Research Intervention

This research will involve a focus group discussion to determine the projected model functional and non-functional requirements.

Participant selection

We are inviting individuals with knowledge in blockchain and cryptocurrencies to participate in the research on coming up with a model that would create a stable cryptocurrency using fiat currency to promote global electronic commerce.

Voluntary Participation

Your participation in this research is entirely voluntary. It is your choice whether to participate or not. Whether you choose to participate or not, all the services you (currenctly or future intent to) receive (if any) at Kabarak University will continue and nothing will change.

Duration

The research takes place over four months. During that time, you will help in defining the potential fuctional and non-functional requirement at te beginning of the research. At the end of the research, it will be necessary for you to participate in model validation. In total, we will meet you two times (during model design and model validation)

Benefits

There may not be any benefit for you but your participation is likely to help us find the answer to the research question(s). There may not be any benefit to the society at this stage of the research, but future generations are likely to benefit.

Confidentiality

The information that we collect from this research project will be kept confidential. Information about you that will be collected during the research will be put away and no-one but the researchers will be able to see it. Any information about you will have a focus group number and unique ID on it instead of your

name. Only the researchers will know what your unique ID or focus group is. It will not be shared with or given toanyone except Prof. Simon Karume and Dr. Nelson Masese who are part of this research team.

Sharing the Results

The knowledge that we get from doing this research will be shared with during our last meeting meeting before it is made widely available to the public. Confidential information will not be shared. After the last meeting, we will publish the results in order that other interested people may learn from our research.

Right to Refuse or Withdraw

You do not have to take part in this research if you do not wish to do so. You may also stop participating in the research at any time you choose. It is your choice and all of your rights will still be respected

Who to Contact

If you have any questions you may ask them now or later, even after the study has started. If you wish to ask questions later, you may contact any of the following:

1. Alex Kibet
   alexkibet@kabarak.ac.ke
   0717470102
2. Prof. Simon Karume
   skarume@kabarak.ac.ke
   0722499397
3. Dr. Nelson Masese
   NMasese@kabarak.ac.ke
   0727171725

PART II: CERTIFICATE OF CONSENT

I have read the foregoing information. I have had the opportunity to ask questions about it and any questions that I have asked have been answered to my satisfaction. I consent voluntarily to participate as a participant in this research.

Name _____ Signature_____Date _____

Day/month/year

I have witnessed the accurate reading of the consent form to the potential participant, and the individual has had the opportunity to ask questions. I confirm that the individual has given consent freely.

Name _____ Signature_____Date _____

Day/month/year

Statement by the researcher/person taking consent

I have accurately read out the information sheet to the potential participant, and to the best of my ability made sure that the participant understands that the following will be done:

1. *Participation in this research is entirely voluntary*
2. *The information to be collected from this research project will be kept confidential*
3. *Knowledge gained from the research will be shared during the last meeting before it is made widely available to the public*
4. **..**
5. **..**
6. *….(if any other that may arise arises)*

I confirm that the participant was given an opportunity to ask questions about the study, and all the questions asked by the participant have been answered correctly and to the best of my ability.

I confirm that the individual has not been coerced into giving consent, and the consent has been given freely and voluntarily.

A copy of this ICF has been provided to the participant.

Name_____Signature_____Date _____

Day/month/year

A**PPENDIX II:** Inform Consent Procedures

Inform consent procedures For Use during the research entitled 'A Model for Creating Stable Cryptocurrency Using Fiat Currency for Global Electronic Commerce' (Adapted from DAIDS Version 1.0)

Purpose

To describe the process of obtaining informed consent from the potential study participant.

Introduction

Informed consent is an on-going process and starts at the initial contact with the potential participant and continues throughout the entire follow-up period of the study. To ensure voluntary expression of the consent by a subject and the adequate information disclosure about the research and essential elements of the informed consent process, researcher should have a clear procedure. This document will guide the procedure to obtain informed consent for the envisioned research.

Procedures

1. All materials used for obtaining informed consent and verbal discussions are in a language understandable by the participant (English)
2. Investigators obtain informed consent using the latest version of the KUREC-approved Informed Consent Form (ICF).
3. Participants are offered the opportunity to take the ICF home to read and return on another day to complete the informed consent process, **if needed**.
4. An introductory letter from the Institute of postgraduate studies (IPGS) of Kabarak University, ethical clearance obtained from Kabarak University Research Ethics Committee (KUREC),

and a research permit obtained from the National Commission for Science Innovation, and Technology (NACOSTI), will be provided to the potential participant.

5. To obtained the consent, the following will be conducted for the informed consent process***:***

5.1. The researcher will provide a copy of the ICF and allow the participant to read it.

5.2. Review the ICF with the participant, addressing each separate section of the ICF, highlighting the main points, and allowing and encouraging the participant to ask questions or express any concerns he/she may have. Briefly document the participant's questions and answers provided in the research record. Use the Informed consent support materials as applicable.

5.3. After all IC materials have been reviewed, and all participant questions/concerns have been addressed, verify that the participant understands the study and ICF elements. (a checklist for verification is marked)

5.3.1. As part of the process of assessing the participant's understanding of the research, clarify any incorrect responses; provide correct information and other explanations.

5.3.2. For participants who are not able to understand all the required information, give the consent form to the participant to take home and read and schedule him/her for another visit date. If, after all efforts, he/she is unable to understand the required information, he/she is ineligible for the study.

5.4. If the participant demonstrates that he/she fully understands the material in the ICF, and if he/she chooses to take part, ask the participant to print his/her name and sign and date the ICF.

5.5. After witnessing the participant's signature, the person facilitating the informed consent process should print his/her own full name, date, and sign the ICF. All signature and date blocks included on the ICF must be completed by the applicable signatory.

6. Documentation requirements of the informed consent process, as well as providing the participant the completed informed consent form.

6.1. A copy of the signed ICF is offered to the participant and the original is kept on file in a confidential manner in the IPGS of Kabarak university

6.2. No study procedures will be done prior to obtaining informed consent from the participant. The date documented on the ICF must either precede or coincide with the first date of study procedures.

6.3. The signed ICF will be considered a permanent part of the participant's record but should be filed separately from the participant's study binder in order to protect confidentiality.

7. Ongoing Informed Consent Procedures

7.1.The informed consent will be valid until the end of the research as indicated in the ICF element "duration". The principle investigator should ensure that the study procedure is completed and communicated as captured in the ICF.

List of Abbreviations and Acronyms

ICF	Informed Consent Form
KUREC	Kabarak University Research Ethics Committee
NACOSTI	National Commission for Science Innovation, and Technology
IPGS	Institute of Postgraduate Studies
IC	Informed Consent

APPENDIX III: Enrollment Informed Consent Comprehension Checklist

ENROLLMENT INFORMED CONSENT COMPREHENSION CHECKLIST			
Name or PTID: ……		**Date:**	**…….**
INSTRUCTIONS: Ask each question and then check each item that participants understand during the discussion without a detailed explanation of the correct answer. While running the checklist, you can provide additional explanations for the question and validation of the answers, but additional explanations for the correct answer should only be provided after the entire checklist is complete. After completing the checklist, provide explanation / advice for items that participants cannot prove their understanding, but please do not check these items. Instead, use comment columns to document follow-up discussions and results. If you check the item, the comment category a or b will be displayed. For unchecked items, comment category c is normally displayed, but category d may also be displayed.			

Open-Ended Question/Statement		**Required Points of Comprehension**	✓	**Comments**
1	**Please describe your understanding of the purpose of the study.**	a. Developing a model for creating stable cryptocurrency		
		validating the model for creating stable cryptocurrency		

2	**Please tell me why you were selected as a possible participant in this study**	Because of my experience		
		b. I am good in blockchain application development		
3	**What are participants being asked to do in this study?**	a. to define the envisioned model requirements		
4	**What is the purpose of this study?**	a. Improvement of cryptocurrency and blockchain		
5	**how is the participation in this study?**	a. participation in this research is entirely voluntary		
6	**What are the benefits of participating in this study?**	a. future benefits should be mentioned		
7	**what is the research duration?**	a. 4 weeks		
8	**What should participants do if they have questions or concerns about what is happening in the study?**	a. ask questions direct or through the given contacts		
9	**What are the possible benefits for participants in the study?**	a. Information about participants is confidential, and private		
		b. Only people working on the study have access to her information		

10	**how will this research share knowledge gained?**	a. during the last meeting		
		b. private information will not be shared		

OUTCOME:

- ◯ Demonstrated comprehension of all required points, decided to enroll in study.
- ◯ Demonstrated comprehension of all required points, decided NOT to enroll in study.
- ◯ Demonstrated comprehension of all required points, deferred enrollment decision.
- ◯ Did not demonstrate comprehension of all required points (yet), needs more time/discussion.
- ◯ Unable to demonstrate comprehension of all required points, consent process discontinued.
- ◯ Other (specify):_____

Optional Comment Codes:

a. Answered correctly on first try
b. Could not answer at first but answered correctly with probing
c. Answered incorrectly at first but answered correctly after discussion
d. Not able to answer correctly at this time
e. Other (describe)…… ……..

Researcher Signature: ……

APPENDIX IV: 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.

FOCUS GROUP INTRODUCTION

Welcome

Thanks for agreeing to be part of the focus group. We appreciate your willingness to participate.

Introductions

Moderator and assistant moderator…

Purpose of Focus Groups

We are building a model for creating stable cryptocurrency. The reason we are having these focus groups is to out define the model requirements. We need your input and want you to share your honest and open thoughts with us.

Ground Rules

1. ***We Want You To Do The Talking***. We would like everyone to participate. I may call on you if I have not heard from you in a while.

2. **There Are No Right Or Wrong Answers** Every person's experiences and opinions are important. Speak up whether you agree or disagree. We want to hear a wide range of opinions.

3. **What Is Said In This Room Stays Here** We want folks to feel comfortable sharing when sensitive issues come up.

4. **We Will Be Tape Recording The Group** We want to capture everything you have to say. We don't identify anyone by name in our report. You will remain anonymous.

Engagement questions:

1. What is your favorite Chain?

2. What do you notice when you look at smart contract code?

3. What is your favorite bridge?

4. What is your best wallet?

System requirements:

1. As an admin of a smart contract system, what would you want?
2. As a model user, what would you want?
3. What type of user experience would you want?
4. How would you design a smart contract?

APPENDIX V: Sample Letter to Request for Permission to Conduct Research

16/11/2021

Alex Kibet

P.O Box 1100,

Nyahururu.

Mobile No: 0717470102

Email: alexriongosha@gmail.com

THE MANAGING DIRECTOR

(ABC…. Company)

Dear Sir/Madam

REQUEST FOR PERMISSION TO CONDUCT RESEARCH IN YOUR INSTITUTION

My name is Alex Kibet, and I am a Ph.D. candidate at Kabarak University. The research I wish to conduct for my Doctoral thesis involves the development of a model for Creating Stable Cryptocurrency Using Fiat Currency for Global Electronic Commerce. This project will be conducted under the supervision of Prof. Simon Karume (kabarak University) and Dr. Nelson Masese (kabarak university).

I am hereby seeking your consent to approach a number of employees in your institution to participate in this project.

I have provided you with a copy of my research proposal which includes the consent form and guidelines to be used during the research process. I have also provided an approval letter which I received from Kabarak university Research Ethics Committee (KUREC) and also a permit obtained from the National Commission for Science Innovation and Technology (NACOSTI).

Upon completion of the study, I will provide you with a bound copy of the full research report. If you require any further information, please do not hesitate to contact me on: 0717470102/ alexriongosha@gmail.com.

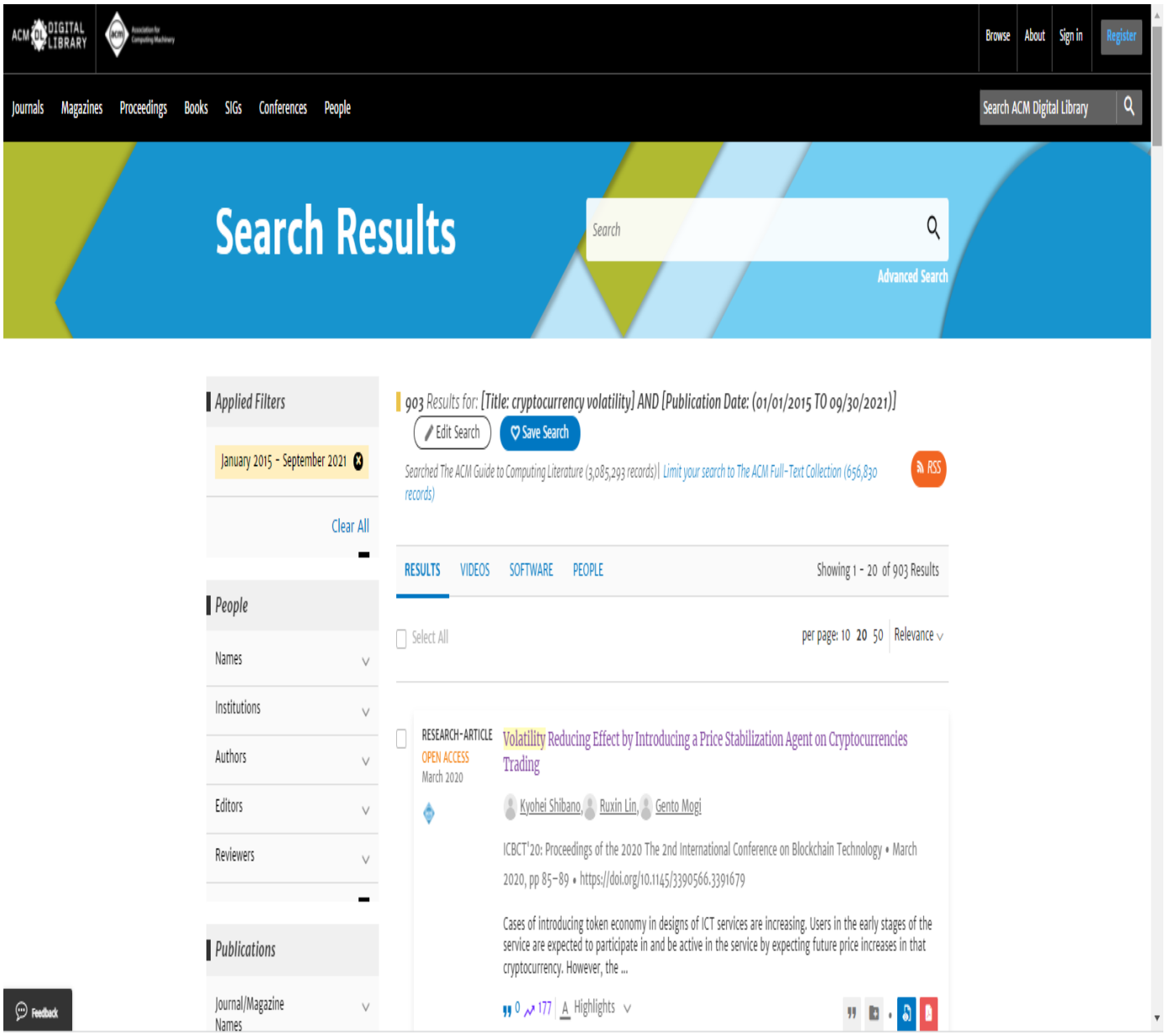
Thank you for your time and consideration in this matter.

Yours sincerely,

Alex kibet

Kabarak University

APPENDIX VI: Integrative Literature Review Search Results



APPENDIX VII: Pilot Testing Material

Introduction

This model creates a stable cryptocurrency using fiat currency for global electronic commerce is research work. The purpose of your participation in this research is to help the researcher in testing model functionalities and the user experience.

System Demonstration

i. User registration
ii. Cryptocurrency creation
iii. Cryptocurrency transfer
iv. Cryptocurrency withdrawal
v. Cryptocurrency exchange
vi. e-commerce operation

Before users can access the system functionalities, they first register. Users register by providing their name and phone number. Upon accessing the system, users can create cryptocurrency by depositing a fiat currency from either a debit card (from GT bank) or mobile money provider (M-pesa). Upon successful deposits, the cryptocurrency will be sent to the user's cryptocurrency account. The user can use the cryptocurrency in various ways.

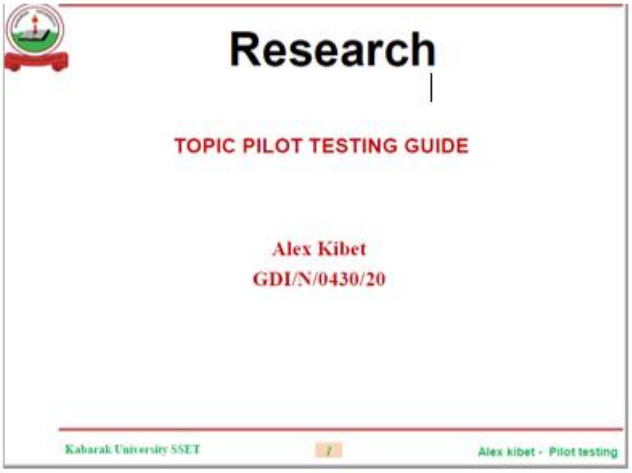
Firstly, a user would use cryptocurrency to pay for goods and services. To demonstrate this functionality a Non-Fungible Tokens (NFT) in the e-commerce module.

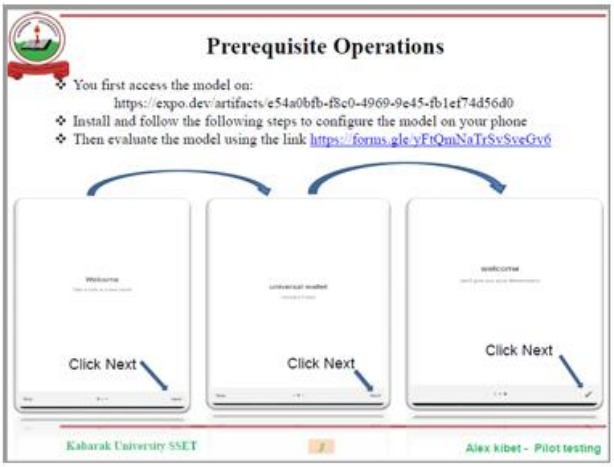
Secondly, could also transfer cryptocurrencies to another account in the transfer module. Here the user specifies the phone number of the receiver. For this to be successful, the receiver’s phone number should be registered with the model.

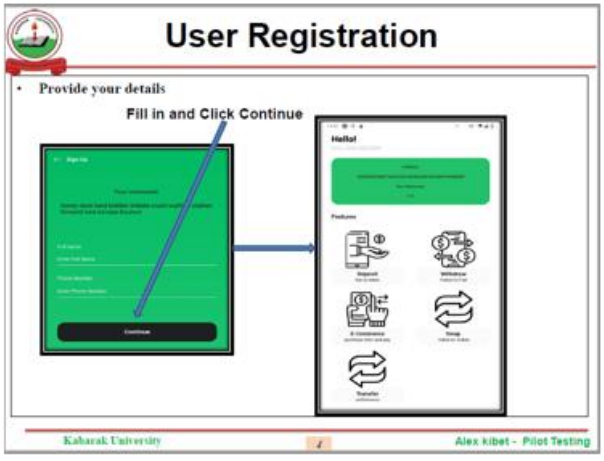
Thirdly, a user can exchange their cryptocurrency from one currency to another (example based on Kenya shilling to Uganda shilling).

Lastly, a user can also take off his or her cryptocurrencies out of the chain using the withdraw module.

The following shows the model screenshots to describe each of these processes.







The users post usage feedback

Access the model on:

https://exp-shell-app-assets.s3.us-west-1.amazonaws.com/android/%40grandmullah/KENCOIN-2400474c6b2445eaaac9dae6a7f0c61c-signed.apk and provide your judgment through the following questions.

PART 1 General Feedback

1. Name _____
2. Mobile Number_____
3. Were you okay with the fact that your details were needed to create a blockchain-based platform? ◯**No** ◯**Yes**
4. Did you like the fact that your mobile money/debit card was linked with the blockchain-based platform? ◯**No** ◯**Yes**
5. Were you able to create a cryptocurrency? ◯**No** ◯**Yes**
6. Were you able to use your cryptocurrency? ◯**No** ◯**Yes**
7. Were you able to buy any NFTs? ◯**No** ◯**Yes**
8. Were you able to change your cryptocurrency from one currency to another? ◯**No** ◯**Yes**
9. Were you able to withdraw your cryptocurrency? ◯**No** ◯**Yes**
10. What did you like most about the system?_____
    _____
    _____
11. What did you not like about the model? _____
    _____
    _____
12. How did you find the system? Easy to use or complicated? _____
    _____
    _____
13. In the event this model is put into full deployment, would you like to continue using it? ◯**No** ◯**Yes**

14. Would you pay to use this system? ◯**No** ◯**Yes**

15. How would you pay for it? _____

_____

PART 2. Evaluation of the model Quality based on the six ISO 9126 quality attributes

A. Functionality Metric

On a scale of 1 to 5, to what extent do you agree to the following statements based on your interaction with the model for creating a stable cryptocurrency for global electronic commerce

(ANSWERS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree)

Sub-Characteristics	**Declaration/ Statement**	**Scores**				
		1	**2**	**3**	**4**	**5**
a) Accuracy	i.) The model was able to provide accurate results for every functionality					
b) Suitability	ii.) The functionalities and help tools provided were sufficient in helping me complete my interaction					
c) Compliance	iii.) The model has all key functions and capabilities I expect it to have					

B. Reliability metric

On a scale of 1 to 5, to what extent do you agree to the following statements based on your interaction with the model for creating a stable cryptocurrency for global electronic commerce **(ANSWERS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree)**

Sub-Characteristics	Declaration/ Statement	Scores				
		1	2	3	4	5
a) Maturity	i.) The model has a good design					
	ii.) The model has a verifiable implementation					
b) Recoverability	iii.) The model is able to recover from errors					
c) Fault tolerance/ availability	iv.) The model functionalities are readily available for use by any registered user					

C. Usability Metric

On a scale of 1 to 5, to what extent do you agree to the following statements based on your interaction with the model for creating a stable cryptocurrency for global electronic commerce **(ANSWERS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree)**

Sub-Characteristics	Declaration/ Statement	Scores				
		1	2	3	4	5
a) Learnability	i.) It was simple to learn and use the model					
	ii.) The information display is clear					
	iii.) The use of words was nonambiguous					
b) Efficiency	i.) Using this model, tasks were quickly completed					

c) Errors	i.)	The model provides clear information on how to fix error problems when they occur					
d) Memorability	i.)	It was easy to get re-established to the model even after long period of not using it					
e) Attractiveness	i.)	The model has an enjoyable interface					
	ii.)	The model has consistent use of colors					
	iii.)	I love the use of symbols and conventions in this model					
f) Subjective Satisfaction	i.)	I feel comfortable using this model					
	ii.)	I feel empowered with this model					
	iii.)	Overall, I am satisfied with this model performance					

D. Efficiency Metric

On a scale of 1 to 5, to what extent do you agree to the following statements based on your interaction with the model for creating a stable cryptocurrency for global electronic commerce **(ANSWERS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree)**

Sub-Characteristics	**Declaration/ Statement**		**Scores**				
			1	**2**	**3**	**4**	**5**
a) Time behavior	i.)	The model performance is time responsive and satisfying					

b) Resource Utilization	ii.) The model adequately utilizes all its supplied device resources to help effectively perform specified tasks					

E. Maintainability Metric

On a scale of 1 to 5, to what extent do you agree to the following statements based on your interaction with the model for creating a stable cryptocurrency for global electronic commerce **(ANSWERS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree)**

Sub-Characteristics	**Declaration/ Statement**	**Scores**				
		1	**2**	**3**	**4**	**5**
i.) Analyzability	i.) The model can be diagnosed to identify areas for improvement					
	ii.) The model can be operated and fault identified					
ii.) Changeability	i.) The model can be modified to make it more resilient without compromising its goal					
	ii.) A new feature can be added to this model					
iii.) Testability	iii.) The model functionalities can effectively and efficiently be performed					
Overall, I would recommend this model to colleagues or contacts within private and public sectors for business or other purposes						

F. Portability Metric

On a scale of 1 to 5, to what extent do you agree to the following statements based on your interaction with the model for creating stable cryptocurrency for global electronic commerce **(ANSWERS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree)**

Sub-Characteristics	Declaration/ Statement	Scores				
		1	2	3	4	5
a) Adaptability	i.) The model can adapt to future changes					
	ii.) The model can accommodate new features					
b) Installability	i.) I was able to download and install the model					
	ii.) The model installation was successful					
c) Co-existence	i.) The model was able to run on my device without affecting operations of other applications					
d) Replaceability	i.) The model components can be replaced					

APPENDIX VIII: Nacosti Research License

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **446826**

Date of Issue: **15/November/2021**

RESEARCH LICENSE

This is to Certify that Mr.. alex kibet of Kabarak University, has been licensed to conduct research in Nairobi, Nakuru on the topic: A MODEL FOR CREATING A STABLE CRYPTOCURRENCY USING FIAT CURRENCY FOR GLOBAL ELECTRONIC COMMERCE for the period ending : 15/November/2022.

License No: **NACOSTI/P/21/14117**

446826

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.

THE SCIENCE, TECHNOLOGY AND INNOVATION ACT, 2013

The Grant of Research Licenses is Guided by the Science, Technology and Innovation (Research Licensing) Regulations, 2014 CONDITIONS

1. The License is valid for the proposed research, location and specified period
2. The License any rights thereunder are non-transferable
3. The Licensee shall inform the relevant County Director of Education, County Commissioner and County Governor beforecommencement of the research
4. Excavation, filming and collection of specimens are subject to further necessary clearence from relevant Government Agencies
5. The License does not give authority to tranfer research materials
6. NACOSTI may monitor and evaluate the licensed research project
7. The Licensee shall submit one hard copy and upload a soft copy of their final report (thesis) within one year of completion of theresearch
8. NACOSTI reserves the right to modify the conditions of the License including cancellation without prior notice

National Commission for Science,

Technology and

Innovationoff Waiyaki

Way, Upper Kabete,

P. O. Box 30623, 00100 Nairobi, KENYA

Land line: 020 4007000, 020 2241349, 020 3310571, 020 8001077

Mobile: 0713 788 787 / 0735 404 245

E-mail: dg@nacosti.go.ke

/

registry@nacosti.go.keW

ebsite: www.nacosti.go.ke

APPENDIX IX: Ethical Clearance

KABARAK UNIVERSITY RESEARCH ETHICS COMMITTEE

Private Bag - 20157
KABARAK, KENYA
Email: kurec@kabarak.ac.ke

Tel: 254-51-343234/5
Fax: 254-051-343529
www.kabarak.ac.ke

OUR REF: KABU01/KUREC/001/1/11/21

Date: 1st Nov, 2021

Alex Kibet,
Kabarak University,

Dear Alex,

RE: A MODEL FOR CREATING A STABLE CRYPTOCURRENCY USING FIAT CURRENCY FOR GLOBAL ELECTRONIC COMMERCE

This is to inform you that ***KUREC*** has reviewed and approved your above research proposal. Your application approval number is ***KUREC-11121.*** The approval period is ***1/11/2021 – 1/11/ 2022.***
This approval is subject to compliance with the following requirements:

i. The researcher (post-graduate) shall obtain a RESEARCH PERMIT from NACOSTI before commencement of data collection & submit a copy to the Kabarak University Institute of Postgraduate Studies (IPGS). All other applicants shall submit a copy of the permit to **KUREC**
ii. Only approved documents including (informed consents, study instruments, MTA Material Transfer Agreement) will be used
iii. All changes including (amendments, deviations, and violations) are submitted for review and approval by ***KUREC***:
iv. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to ***KUREC*** within 72 hours of notification;
v. Any changes, anticipated or otherwise that may increase the risk(s) or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to ***KUREC*** within 72 hours;
vi. Clearance for export of biological specimens must be obtained from relevant institutions and submit a copy of the permit to KUREC;
vii. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal and;
viii. Submission of an executive summary report within 90 days upon completion of the study to ***KUREC***

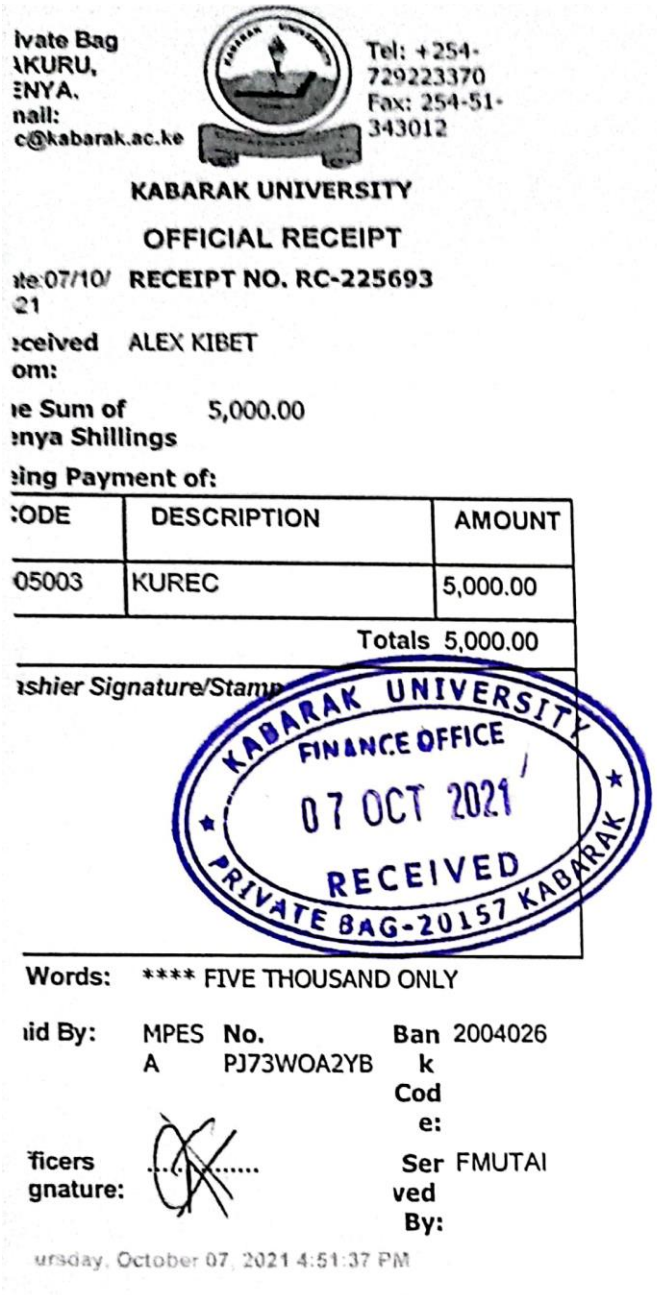
Sincerely,

Prof. Jackson Kitetu PhD.
KUREC-Chairman

KABARAK UNIVERSITY
INSTITUTIONAL RESEARCH ETHICS COMMITTEE
01 NOV 2021
APPROVED
P. O. PRIVATE BAG - 20157, KABARAK

Cc Vice Chancellor
DVC-Academic & Research
Registrar-Academic & Research
Director-Research Innovation & Outreach
Institute of Post Graduate Studies

APPENDIX X: Kurec Official Receip



ivate Bag
KURU,
ENYA.
nail:
c@kabarak.ac.ke

Tel: +254-729223370
Fax: 254-51-343012

KABARAK UNIVERSITY

OFFICIAL RECEIPT

ite:07/10/21 **RECEIPT NO. RC-225693**

ceived om: ALEX KIBET

ie Sum of enya Shillings 5,000.00

eing Payment of:

CODE	DESCRIPTION	AMOUNT
05003	KUREC	5,000.00
	Totals	5,000.00

ashier Signature/Stamp

KABARAK UNIVERSITY
FINANCE OFFICE
07 OCT 2021
RECEIVED
PRIVATE BAG-20157 KABARAK

Words: **** FIVE THOUSAND ONLY

aid By: MPESA No. PJ73WOA2YB Bank Code: 2004026

fficers gnature: ..... Served By: FMUTAI

ursday, October 07, 2021 4:51:37 PM

APPENDIX XI: Institute of Post Graduate Studies Letter for Nacosti

KABARAK UNIVERSITY
OFFICE OF THE DIRECTOR
INSTITUTE OF POST GRADUATE STUDIES

Private Bag - 20157
KABARAK, KENYA
http://kabarak.ac.ke/institute-postgraduate-studies/
E-mail: directorpostgraduate@kabarak.ac.ke

2nd November 2021

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

Dear Sir/Madam,

RE: ALEX KIBET-GDI/N/0430/01/20

The above named is a student at Kabarak University. He is carrying out a research entitled "***A model for creating a stable cryptocurrency using fiat currency for global electronic commerce***".

The student has been granted ethical clearance by Kabarak University Research Ethics Committee and is ready to undertake field research.

Kindly provide the student with a research permit to enable him to undertake the research.

Thank you.

KABARAK UNIVERSITY
DIRECTOR
POST GRADUATE STUDIES
02 NOV 2021
PRIVATE BAG - 20157, KABARAK

Dr. Wilson O. Shitandi
DIRECTOR, INSTITUTE OF POST GRADUATE STUDIES

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

Kabarak University is ISO 9001:2015 Certified

APPENDIX XII: Model Core Source Code

APP Contract

```
pragma solidity >=0.6.0 <0.9.0;
import './USD.sol';
  USD Token;
  bytes32 public constant DEPOSIT_ROLE = keccak256("DEPOSIT_ROLE");
  bytes32 public constant ADMIN_ROLE = keccak256("ADMIN_ROLE");
  bytes32 public constant RELAYER_ROLE = keccak256("RELAYER_ROLE");
  constructor ( USD _Token,address _owner) public {
    Token = _Token;
    _setupRole(DEFAULT_ADMIN_ROLE, _owner);
    _setupRole(DEPOSIT_ROLE, _owner);
    _setupRole(ADMIN_ROLE,_owner);
    _setupRole(RELAYER_ROLE,_owner);  }
  event LogNewQuery(string identity,uint256 amount , bytes32 id );
  event LogErrorInCallback(string description);
  event newDeposit(bytes32 id ,string result);
  event newWithdrawal(string result, uint256 amount);
  struct Queuevalues {
    uint256 amount;
    address sender;
    State state;  }
  enum State {pending,completed}
  modifier depositState(bytes32 _Id, State _state){
    require(TxQueue[_Id].state == _state,'transaction already completed');    _;  }
  struct Agent {
    string details;
    uint256 value;
    State state;  }
  mapping (bytes32 =>Queuevalues)public TxQueue;
  mapping (bytes32 =>Agent)private AgentDetails;
```

```
  mapping (address => uint256) public replayNonce;
  function _query(address _sender, string memory identity, uint256 _amount)public view returns(bytes32 _id)  {
  return keccak256(abi. EncodePacked(_sender, identity, _amount,block. Timestamp));  }
  function _callback(bytes32 _myid,string memory _result,uint8 _status )
  public  virtual  depositState(_myid,State.pending)
  {
Require(hasRole(DEPOSIT_ROLE, _msgSender()), "PESA: must have minter role to Deposit");
    Queuevalues storage Que = TxQueue[_myid];
    if(_status == uint8(0) ){
      uint256 amount =  Que.amount;
      address  _to =  Que.sender;
      Token.Transfer(_to,amount);
      Que.state = State.completed;
      emit newDeposit(_myid,_result);
    }else{
      emit LogErrorInCallback(_result);
      Que.state= State.completed;   }   }
    function deposit(
    bytes memory signature,
    string memory identity,
    uint256 amount,
    uint256  nonce     )
     public  virtual
    {
    Require (hasRole (RELAYER_ROLE, _msgSender()), "ERC20relayer: must have relayer role to relay tx");
    bytes32 meta_Hash = metaHash(identity,amount,nonce,"metaDeposit");
    address signer = getSigner(meta_Hash,signature);
    bytes32  Request_Id = _query(signer,identity,amount);
    //make sure signer doesn't come back as 0x0
```

```
    require(signer!=address(0));
    require(nonce == replayNonce[signer],"Attack: this is a replay attack ");
    replayNonce[signer]++;
    require(Token.balanceOf(address(this)) > amount,'insufficient funds');
    Queuevalues storage Que = TxQueue[Request_Id];
    Que.sender = signer;
    Que.amount = amount;
    Que.state = State.pending;
    emit LogNewQuery( identity , amount, Request_Id); }
    function b2cCallback(uint _status, string memory _result, uint256 txcost,  uint256 amount, address user) public virtual{
    require(hasRole(ADMIN_ROLE, _msgSender()), "ERC20relayer: must have relayer role to relay tx");
    if(_status == uint(0)){
     require(Token. TransferFrom(user,address(this),amount));
        emit newWithdrawal(_result,amount);
    }else{
          emit LogErrorInCallback(_result);
    }  }
  function creditTo(address _user, uint256 amount, bytes memory signature, uint256 nonce)public virtual {
    bytes32 meta_Hash = metaHash('transfer',amount,nonce,"metaCredit");
    address signer = getSigner(meta_Hash,signature);
    //make sure signer doesn't come back as 0x0
    require(signer!=address(0));
    require(nonce == replayNonce[signer],"Attack: this is a replay attack ");
    replayNonce[signer]++;
    require(hasRole(ADMIN_ROLE, signer), "pesa: must have admin role to withdraw");
    Token.transfer(_user,amount);
  }
```

```
  function metaHash(string memory identity, uint256 value, uint256 nonce ,string memory metamethod) public view returns(bytes32){
    return keccak256(abi. EncodePacked(address(this),metamethod, identity, value, nonce));
  }
  function getSigner(bytes32 _hash, bytes memory _signature) internal pure returns (address){
    bytes32 r;
    bytes32 s;
    uint8 v;
    if (_signature.length != 65) {
        return address(0);
    }
    assembly {
        r := mload(add(_signature, 32))
        s := mload(add(_signature, 64))
        v := byte(0, mload(add(_signature, 96)))
    }
    if (v < 27) {
        v += 27;
    }
    if (v != 27 && v != 28) {
        return address(0);
    } else {
    return ecrecover(keccak256(
        abi. EncodePacked("\x19Ethereum Signed Message:\n32", _hash)
    ), v, r, s);    }  } }
```

Ecommerce contract

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
pragma experimental ABIEncoderV2;
contract Comerce {
```

```
  struct BoredApe{
    uint id;
    string name;
    address owner;
    uint256 price;
    string description;  }
  mapping (uint => BoredApe) public Apes;
     uint public memberCount;
 function addApe(string calldata _name, address _owner, string calldata _des,uint256   _price)
public {
    Apes[memberCount] = BoredApe(memberCount,_name,_owner, _price,_des);
    memberCount++;   }
  //0x9E5d7363fC8B1551fB2899DE33Bad6c27A08aF39
  function getApes() public view returns (uint[] memory, string[] memory,address[]
  memory , string[] memory ,uint256[] memory){
      uint[]    memory id = new uint[](memberCount);
      string[]  memory name = new string[](memberCount);
      address[] memory owner = new address[](memberCount);
      string[]    memory description = new string[](memberCount);
      uint256[]    memory price = new uint256[](memberCount);
      for (uint i = 0; i < memberCount; i++) {
          BoredApe storage ape = Apes[i];
Id[i] = ape.id;
Name[i] = ape.name;
Owner[i] = ape.owner;
Description[i] = ape.description;
Price[i] =ape.price;      }
      return (id, name,owner,description,price);  }
  function sellApe (uint _id,address new_owner ) public {
      BoredApe storage ape = Apes[_id];
      ape.owner = new_owner;  } }
```

ENS contract

```
// SPDX – License-Identifier: MIT
pragma solidity 0.8.2;
// pragma experimental ABIEncoderV2
contract ENS {
    mapping (address => string) public ens;
    mapping (uint256 => address) public phoneNumber;
    address[]  public users;
    function registername( string calldata name, uint256 _No ,bytes memory signature) public {
        bytes32 meta_Hash = metaHash(name);
        address signer = getSigner(meta_Hash,signature);
       ens[signer] = name;
       phoneNumber[_No] = signer;
       users.push(signer);    }
    function getUsers() public view returns(address[] memory){
        return users;    }
    function metaHash(string memory metadetails) public pure  returns(bytes32){
        return keccak256(abi. EncodePacked(metadetails));    }
    function getSigner(bytes32 _hash, bytes memory _signature) internal pure returns (address){
        bytes32 r;
        bytes32 s;
        uint8 v;
        if (_signature.length != 65) {
            return address(0);        }
        assembly {
            r := mload(add(_signature, 32))
            s := mload(add(_signature, 64))
            v := byte(0, mload(add(_signature, 96)))        }
        if (v < 27) {
            v += 27;        }
        if (v != 27 && v != 28) {
```

```
        return address(0);
    } else {
    return ecrecover(keccak256(
        abi.encodePacked("\x19Ethereum Signed Message:\n32", _hash)
    ), v, r, s);        }    }  }
```

SWAP Contract

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.7.0;
import "./usd.sol";
contract Swap  {
   using SafeMath for uint256;
   mapping (address => uint256) public exchangeRates;
   event swapping (
      address user,
      string from,
      string to,
      uint256 amount     );
   function setExchange (address token , uint256 price) public  {
      exchangeRates[token] = price;     }
   function swap ( address _tokenFrom ,address _tokenTo , uint256 amount, bytes memory
signature) public {
      bytes32 meta_Hash = metaHash(_tokenFrom,_tokenTo,amount);
      address signer = getSigner(meta_Hash,signature);
     uint256 fromRate = exchangeRates[_tokenFrom];
     uint256 toRate = exchangeRates[_tokenTo];
      require(USD(_tokenFrom).transferFrom(signer ,address(this),amount));
      uint256 base  = amount.div(fromRate);
      uint256 receiveAmount = base.mul(toRate);
      USD(_tokenTo).transfer(signer,receiveAmount);
     emit swapping (signer,USD(_tokenFrom).symbol(),USD(_tokenTo).symbol(),amount); }
```

```
    function metaHash(address _tokenFrom ,address _tokenTo , uint256 amount) public pure returns(bytes32){
        return keccak256(abi.encodePacked(_tokenFrom,_tokenTo,amount));     }
    function getSigner(bytes32 _hash, bytes memory _signature) internal pure returns (address){
        bytes32 r;
        bytes32 s;
        uint8 v;
        if (_signature.length != 65) {
            return address(0);           }
        assembly {
            r := mload(add(_signature, 32))
            s := mload(add(_signature, 64))
            v := byte(0, mload(add(_signature, 96)))
        }
        if (v < 27) {
            v += 27;        }
        if (v != 27 && v != 28) {
            return address(0);
        } else {
        return ecrecover(keccak256(
            abi.encodePacked("\x19Ethereum Signed Message:\n32", _hash)
        ), v, r, s); }     } }
```

SWAP B

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.6.0 <0.9.0;
interface IERC20 {
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address recipient, uint256 amount) external returns (bool);
    function allowance(address owner, address spender) external view returns (uint256);
```

```
    function approve(address spender, uint256 amount) external returns (bool);
    function transferFrom(address sender, address recipient, uint256 amount) external returns (bool);
    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value); }
library SafeMath {
    function add(uint256 a, uint256 b) internal pure returns (uint256) {
        uint256 c = a + b;
        require(c >= a, "SafeMath: addition overflow");
        return c;     }
    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
        return sub(a, b, "SafeMath: subtraction overflow");    }
    function sub(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
        require(b <= a, errorMessage);
        uint256 c = a - b;
        return c; }
    function mul(uint256 a, uint256 b) internal pure returns (uint256) {
        // Gas optimization: this is cheaper than requiring 'a' not being zero, but the
        // benefit is lost if 'b' is also tested.
        // See: https://github.com/OpenZeppelin/openzeppelin-contracts/pull/522
        if (a == 0) {
            return 0; }
        uint256 c = a * b;
        require(c / a == b, "SafeMath: multiplication overflow");
        return c;    }
    function div(uint256 a, uint256 b) internal pure returns (uint256) {
        return div(a, b, "SafeMath: division by zero");    }
        function div(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
        require(b > 0, errorMessage);
```

```
        uint256 c = a / b;
        // assert(a == b * c + a % b); // There is no case in which this doesn't hold
        return c;    }
    function mod(uint256 a, uint256 b) internal pure returns (uint256) {
        return mod(a, b, "SafeMath: modulo by zero");    }
    function mod(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256)
{
        require(b != 0, errorMessage);
        return a % b;     } }
abstract contract Context {
    function _msgSender() internal view virtual returns (address payable) {
        return msg.sender;    }
    function _msgData() internal view virtual returns (bytes memory) {
        this;
        return msg.data;     } }
library Address {
    function isContract(address account) internal view returns (bool) {
        // According to EIP-1052, 0x0 is the value returned for not-yet created accounts
        //    and    0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470is
returned
        // for accounts without code, i.e. `keccak256('')`
        bytes32 codehash;
        bytes32                                    accountHash                                    =
0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470;
        // solhint-disable-next-line no-inline-assembly
        assembly { codehash := extcodehash(account) }
        return (codehash != accountHash && codehash != 0x0);    }
        // and 0 x c 5 d 2 4 6 0 1 8 6 f 7 2 3 3 c 9 2 7 e 7 d b 2 d c c 7 0 3 c 0 e  5 0 0 b 6 5 3 c a 8 2 2
7 3b 7 b f a d 8 0 4 5 d 8 5 a 4 7 0   is returned
    function sendValue(address payable recipient, uint256 amount) internal {
        require(address(this).balance >= amount, "Address: insufficient balance");
```

```
        (bool success, ) = recipient.call{ value: amount }("");
        require(success, "Address: unable to send value, recipient may have reverted");    }
    function functionCall(address target, bytes memory data) internal returns (bytes memory) {
      return functionCall(target, data, "Address: low-level call failed");    }
    function functionCall(address target, bytes memory data, string memory errorMessage) internal
returns (bytes memory) {
        return _functionCallWithValue(target, data, 0, errorMessage);    }
    function functionCallWithValue(address target, bytes memory data, uint256 value) internal
returns (bytes memory) {
        return functionCallWithValue(target, data, value, "Address: low-level call with value
failed");    }
    function functionCallWithValue(address target, bytes memory data, uint256 value, string
memory errorMessage) internal returns (bytes memory) {
        require(address(this).balance >= value, "Address: insufficient balance for call");
        return _functionCallWithValue(target, data, value, errorMessage);    }
    function _functionCallWithValue(address target, bytes memory data, uint256 weiValue, string
memory errorMessage) private returns (bytes memory) {
        require(isContract(target), "Address: call to non-contract");
        (bool success, bytes memory returndata) = target.call{ value: weiValue }(data);
        if (success) {
            return returndata;
        } else {
            // Look for revert reason and bubble it up if present
            if (returndata.length > 0) {
                // The easiest way to bubble the revert reason is using memory via assembly
                // solhint-disable-next-line no-inline-assembly
                assembly {
                    let returndata_size := mload(returndata)
                    revert(add(32, returndata), returndata_size)
                }
            } else {
```

```
            revert(errorMessage);
        }       }    }}
abstract contract AccessControl is Context {
    using EnumerableSet for EnumerableSet.AddressSet;
    using Address for address;
    struct RoleData {
        EnumerableSet.AddressSet members;
        bytes32 adminRole;    }
    mapping (bytes32 => RoleData) private _roles;
    bytes32 public constant DEFAULT_ADMIN_ROLE = 0x00;
    event RoleAdminChanged(bytes32 indexed role, bytes32 indexed previousAdminRole, bytes32
indexed newAdminRole);
    event RoleGranted(bytes32 indexed role, address indexed account, address indexed sender);
    event RoleRevoked(bytes32 indexed role, address indexed account, address indexed sender);
    function hasRole(bytes32 role, address account) public view returns (bool) {
        return _roles[role].members.contains(account);    }
    function getRoleMemberCount(bytes32 role) public view returns (uint256) {
        return _roles[role].members.length();    }
    function getRoleMember(bytes32 role, uint256 index) public view returns (address) {
        return _roles[role].members.at(index);    }
        // and 0 x c 5 d 2 4 6 0 1 8 6 f 7 2 3 3 c 9 2 7 e 7 d b 2 d c c 7 0 3 c 0 e  5 0 0 b 6 5 3 c a 8 2 2
7 3b 7 b f a d 8 0 4 5 d 8 5 a 4 7 0   is returned
   // and 0 x c 5 d 2 4 6 0 1 8 6 f 7 2 3 3 c 9 2 7 e 7 d b 2 d c c 7 0 3 c 0 e  5 0 0 b 6 5 3 c a 8 2 2 7
3b 7 b f a d 8 0 4 5 d 8 5 a 4 7 0   is returned
    function getRoleAdmin(bytes32 role) public view returns (bytes32) {
        return _roles[role].adminRole;
    }
   * 0 x c 5 d 2 4 6 0 1 8 6 f 7 2 3 3 c 9 2 7 e 7 d b 2 d c c 7 0 3 c 0 e  5 0 0 b 6 5 3 c a 8 2 2 7 3b 7
b f a d 8 0 4 5 d 8 5 a 4 7 0   is returned
        // for accounts without code, i.e. `keccak256('')`
    function grantRole(bytes32 role, address account) public virtual {
```

```
        require(hasRole(_roles[role].adminRole, _msgSender()), "AccessControl: sender must be an
admin to grant");
        _grantRole(role, account);
    }
    function revokeRole(bytes32 role, address account) public virtual {
        require(hasRole(_roles[role].adminRole, _msgSender()), "AccessControl: sender must be an
admin to revoke");
        _revokeRole(role, account);    }
    function renounceRole(bytes32 role, address account) public virtual {
        require(account == _msgSender(), "AccessControl: can only renounce roles for self");
        _revokeRole(role, account);    }
    function _setupRole(bytes32 role, address account) internal virtual {
        _grantRole(role, account);    }
    function _setRoleAdmin(bytes32 role, bytes32 adminRole) internal virtual {
        emit RoleAdminChanged(role, _roles[role].adminRole, adminRole);
        _roles[role].adminRole = adminRole;    }
    function _grantRole(bytes32 role, address account) private {
        if (_roles[role].members.add(account)) {
            emit RoleGranted(role, account, _msgSender());
        }    }
    function _revokeRole(bytes32 role, address account) private {
        if (_roles[role].members.remove(account)) {
            emit RoleRevoked(role, account, _msgSender());
        }    }}
library EnumerableSet {
    struct Set {
        bytes32[] _values;
                mapping (bytes32 => uint256) _indexes;    }
    function _add(Set storage set, bytes32 value) private returns (bool) {
        if (!_contains(set, value)) {
            set._values.push(value);
```

```
            set._indexes[value] = set._values.length;
            return true;
        } else {
            return false;
        }    }
    function _remove(Set storage set, bytes32 value) private returns (bool) {
        // We read and store the value's index to prevent multiple reads from the same storage slot
        uint256 valueIndex = set._indexes[value];
        if (valueIndex != 0) { // Equivalent to contains(set, value)
            // To delete an element from the _values array in O(1), we swap the element to delete with
the last one in
            uint256 toDeleteIndex = valueIndex - 1;
            uint256 lastIndex = set._values.length - 1;
            bytes32 lastvalue = set._values[lastIndex];
            set._values[toDeleteIndex] = lastvalue;
            set._indexes[lastvalue] = toDeleteIndex + 1; // All indexes are 1-based
            set._values.pop();
            delete set._indexes[value];
            return true;
        } else {
            return false;
        }    }
    function _contains(Set storage set, bytes32 value) private view returns (bool) {
        return set._indexes[value] != 0;    }
    function _length(Set storage set) private view returns (uint256) {
        return set._values.length;    }
    function _at(Set storage set, uint256 index) private view returns (bytes32) {
        require(set._values.length > index, "EnumerableSet: index out of bounds");
        return set._values[index];    }
    // AddressSet
    struct AddressSet {
```

```
        Set _inner;    }
    function add(AddressSet storage set, address value) internal returns (bool) {
        return _add(set._inner, bytes32(uint256(value)));
    }
    function remove(AddressSet storage set, address value) internal returns (bool) {
        return _remove(set._inner, bytes32(uint256(value)));    }
    function contains(AddressSet storage set, address value) internal view returns (bool) {
        return _contains(set._inner, bytes32(uint256(value)));    }
    function length(AddressSet storage set) internal view returns (uint256) {
        return _length(set._inner);    }
    function at(AddressSet storage set, uint256 index) internal view returns (address) {
        return address(uint256(_at(set._inner, index)));    }
    // UintSet
    struct UintSet {
        Set _inner;    }
    function add(UintSet storage set, uint256 value) internal returns (bool) {
        return _add(set._inner, bytes32(value));    }
    function remove(UintSet storage set, uint256 value) internal returns (bool) {
        return _remove(set._inner, bytes32(value));    }
    function contains(UintSet storage set, uint256 value) internal view returns (bool) {
        return _contains(set._inner, bytes32(value));    }
    function length(UintSet storage set) internal view returns (uint256) {
        return _length(set._inner);    }
    function at(UintSet storage set, uint256 index) internal view returns (uint256) {
        return uint256(_at(set._inner, index));    }}
contract USD is Context, IERC20,AccessControl {
    using SafeMath for uint256;
    mapping (address => uint256) private _balances;
    mapping (address => uint256) public replayNonce;
    mapping (address => mapping (address => uint256)) private _allowances;
    uint256 private _totalSupply;
```

```
    string private _name;
    string private _symbol;
    uint8 private _decimals;
    bytes32 public constant MINTER_ROLE = keccak256("MINTER_ROLE");
    bytes32 public constant PAUSER_ROLE = keccak256("PAUSER_ROLE");
    bytes32 public constant RELAYER_ROLE = keccak256("RELAYER_ROLE");
    constructor (string memory name, string memory symbol) public {
        address admin = msg.sender;
        _name = name;
        _symbol = symbol;
        _decimals = 18;
        _setupRole(DEFAULT_ADMIN_ROLE, admin);
        _setupRole(MINTER_ROLE,admin);
        _setupRole(PAUSER_ROLE, admin);
        _setupRole(RELAYER_ROLE, admin);    }
    function name() public view returns (string memory) {
        return _name;    }
    function symbol() public view returns (string memory) {
        return _symbol;    }
    function decimals() public view returns (uint8) {
        return _decimals;    }
    function totalSupply() public view override returns (uint256) {
        return _totalSupply;    }
    function balanceOf(address account) public view override returns (uint256) {
        return _balances[account];    }
    function transfer(address recipient, uint256 amount) public virtual override returns (bool) {
        _transfer(_msgSender(), recipient, amount);
        return true;    }
    function metaTransfer(bytes memory signature, address to, uint256 amount, uint256 nonce)
public returns (bool) {
```

```
        require(hasRole(RELAYER_ROLE, _msgSender()), "ERC20relayer: must have relayer role to relay tx");
        bytes32 meta_Hash = metaHash(to,amount,nonce,"metaTransfer");
        address signer = getSigner(meta_Hash,signature);
        //make sure signer doesn't come back as 0x0
        require(signer!=address(0));
        require(nonce == replayNonce[signer],"Attack: this is a replay attack ");
        replayNonce[signer]++;
        _transfer(signer, to, amount);
        return true;    }
    function allowance(address owner, address spender) public view virtual override returns (uint256) {
        return _allowances[owner][spender];    }
    function approve(address spender, uint256 amount) public virtual override returns (bool) {
        _approve(_msgSender(), spender, amount);
        return true;    }
const Wallet = new ethers. Wallet( '1 1 a 6 6 0 6 b 9 6 1 3 a c b 5 0 4 c d 7 c 2 0 2 e a1 7 5 b e 4 8 6 a f 1 d f 3 b 8 0 2 9 a 9 0 a d 9 2 3 e d 3 0 1 a b 9 e 6 ', Provider)
    const usdContract  = new  ethers. Contract ('0 x C 0 9 7 2 d 8 A 3 6 9 b 2 7 F e 5 2 a D 8 8 A 9 8 F c B A 7 8 6 8 8 4 D 1 3 e 4 ', to ke n. ou tp ut .a bi  , Wa ll et )
    const contract = new e thers. Contract ('0 x 4 B F f A 6 a 3 5 a F 7 1 6 e 9 4 0 e 9 a 7  D 1 B 2 9 b 4 4 c A E 9 5 7 8 e 8 b ', en s. outp ut .a bi ,W al le t)
    Funct io n  Me ta Ap pr ov e (b yt e s  m em or y  s I gn at u re , ad d re s s  s pe n d er ,  ui n t 2 5 6 amount,uint256 nonce) public virtual  returns (bool) {
        require(hasRole(RELAYER_ROLE, _msgSender()), "ERC20relayer: must have relayer role to relay tx");
        bytes32 meta_Hash = metaHash(spender,amount,nonce,"metaApprove");
        address signer = getSigner(meta_Hash,signature);
        //make sure signer doesn't come back as 0x0
        require(signer!=address(0));
        require(nonce == replayNonce[signer],"Attack: this is a replay attack ");
```

```
        replayNonce[signer]++;
        _approve(signer, spender, amount);
        return true;    }
    function transferFrom(address sender, address recipient, uint256 amount) public virtual override returns (bool) {
        _transfer(sender, recipient, amount);
        _approve(sender, _msgSender(), _allowances[sender][_msgSender()].sub(amount, "ERC20: transfer amount exceeds allowance"));
        return true;    }
    function MetaTransferFrom(bytes memory signature,address sender, address recipient, uint256 amount,uint256 nonce) public virtual  returns (bool) {
        require(hasRole(RELAYER_ROLE, _msgSender()), "ERC20relayer: must have relayer role to relay tx");
        bytes32 meta_Hash = metaHash(recipient,amount,nonce,"metaTransferFrom");
        address signer = getSigner(meta_Hash,signature);
        //make sure signer doesn't come back as 0x0
        require(signer!=address(0));
        require(nonce == replayNonce[signer],"Attack: this is a replay attack ");
        replayNonce[signer]++;
        _transfer(sender, recipient, amount);
        _approve(sender, signer, _allowances[sender][signer].sub(amount, "ERC20: transfer amount exceeds allowance"));
        return true;    }
    function increaseAllowance(address spender, uint256 addedValue) public virtual returns (bool) {
        _approve(_msgSender(), spender, _allowances[_msgSender()][spender].add(addedValue));
        return true;    }
    function metaIncreaseAllowance(bytes memory signature,address spender, uint256 addedValue, uint256 nonce) public virtual returns (bool) {
        require(hasRole(RELAYER_ROLE, _msgSender()), "ERC20relayer: must have relayer role to relay tx");
```

```
        bytes32 meta_Hash = metaHash(spender,addedValue,nonce,"metaIncreaseAllowance");
        address signer = getSigner(meta_Hash,signature);
        //make sure signer doesn't come back as 0x0
        require(signer!=address(0));
        require(nonce == replayNonce[signer],"Attack: this is a replay attack ");
        replayNonce[signer]++;
        _approve(signer, spender, _allowances[signer][spender].add(addedValue));
        return true;    }
    function decreaseAllowance(address spender, uint256 subtractedValue) public virtual returns (bool) {
        _approve(_msgSender(), spender, _allowances[_msgSender()][spender].sub(subtractedValue, "ERC20: decreased allowance below zero"));
        return true;    }
    function metaDecreaseAllowance(bytes memory signature,address spender, uint256 subtractedValue,uint256 nonce) public virtual returns (bool) {
        require(hasRole(RELAYER_ROLE, _msgSender()), "ERC20relayer: must have relayer role to relay tx");
        bytes32 meta_Hash = metaHash(spender,subtractedValue,nonce,"metaDecreaseAllowance");
        address signer = getSigner(meta_Hash,signature);
        //make sure signer doesn't come back as 0x0
        require(signer!=address(0));
        require(nonce == replayNonce[signer],"Attack: this is a replay attack ");
        replayNonce[signer]++;
        _approve(signer, spender, _allowances[signer][spender].sub(subtractedValue, "ERC20: decreased allowance below zero"));
        return true;    }
    function _transfer(address sender, address recipient, uint256 amount) internal virtual {
        require(sender != address(0), "ERC20: transfer from the zero address");
        require(recipient != address(0), "ERC20: transfer to the zero address");
```

```
        _beforeTokenTransfer(sender, recipient, amount);
        _balances[sender] = _balances[sender].sub(amount, "ERC20: transfer amount exceeds balance");
        _balances[recipient] = _balances[recipient].add(amount);
        emit Transfer(sender, recipient, amount);
    }        function metaHash(address spender, uint256 value, uint256 nonce ,string memory metamethod) public view returns(bytes32){
        return keccak256(abi.encodePacked(address(this),metamethod, spender, value, nonce));
    }
    function _mint(address account, uint256 amount) internal virtual {
        require(account != address(0), "ERC20: mint to the zero address");
        _beforeTokenTransfer(address(0), account, amount);
        _totalSupply = _totalSupply.add(amount);
        _balances[account] = _balances[account].add(amount);
        emit Transfer(address(0), account, amount);
    }
    function _burn(address account, uint256 amount) internal virtual {
        require(account != address(0), "ERC20: burn from the zero address");
        _beforeTokenTransfer(account, address(0), amount);
        _balances[account] = _balances[account].sub(amount, "ERC20: burn amount exceeds balance");
        _totalSupply = _totalSupply.sub(amount);
        emit Transfer(account, address(0), amount);
    }
    function _approve(address owner, address spender, uint256 amount) internal virtual {
        require(owner != address(0), "ERC20: approve from the zero address");
        require(spender != address(0), "ERC20: approve to the zero address");
        _allowances[owner][spender] = amount;
        emit Approval(owner, spender, amount);
    }
    function _setupDecimals(uint8 decimals_) internal {
```

```
        _decimals = decimals_;    }
    function _beforeTokenTransfer(address from, address to, uint256 amount) internal virtual { }
    function burn(uint256 amount) public virtual {
        require(hasRole(MINTER_ROLE, _msgSender()), "ERC20PresetMinterPauser: must have minter role to burn");
        _burn(_msgSender(), amount);
    }
    function burnFrom(address account, uint256 amount) public virtual {
        uint256 decreasedAllowance = allowance(account, _msgSender()).sub(amount, "ERC20: burn amount exceeds allowance");
        _approve(account, _msgSender(), decreasedAllowance);
        _burn(account, amount);
    }
    function mint(address to, uint256 amount) public virtual {
        require(hasRole(MINTER_ROLE, _msgSender()), "ERC20PresetMinterPauser: must have minter role to mint");
        _mint(to, amount);
    }
    function getSigner(bytes32 _hash, bytes memory _signature) internal pure returns (address){
        bytes32 r;
        bytes32 s;
        uint8 v;
        if (_signature.length != 65) {
            return address(0);
        }
        assembly {
            r := mload(add(_signature, 32))
            s := mload(add(_signature, 64))
            v := byte(0, mload(add(_signature, 96)))
        }
        if (v < 27) {
```

```
        v += 27;
    }
    if (v != 27 && v != 28) {
        return address(0);
    } else {
    return ecrecover(keccak256(
        abi.encodePacked("\x19Ethereum Signed Message:\n32", _hash)
    ), v, r, s);        }  }}
```

//M-Pesa withdrawal

```
const { getOAuthToken } = require("./deposit")
const axios = require('axios')
const  { publicEncrypt, constants }  = require( "crypto")
const { resolve } =  require("path")
const { readFileSync } =  require("fs")
const {db} = require('./helpers/firbase')
async function Withdrawal (req) {
     const consumer_key_b2c = process.env.consumer_key_b2c
    const consumer_secret_b2c = process.env.consumer_secret_b2c
    console.log('here',consumer_key_b2c)
    const auth =  await getOAuthToken(consumer_key_b2c,consumer_secret_b2c)
    console .log (auth)  const data = read File Sync ( resolve ( process .env. path));
const privateKey = String(data);    var security =    encrypt String With Rsa PublicKey (process. env. password, privateKey)  console. log(security)  let re = await  withdraw (auth, security, req. amount, req. phone Number, req. address)  return re } async function withdraw (token, security, amount, phone Number, address  ) { try {
            // console.log('hapa',security)
              auth = "Bearer " + token ;
           // send the request
              response = await axios. default. Post ('https: //api.safaricom.co.ke/mpesa/b2c/v1/paymentrequest',{
```

"InitiatorName": `${process.env.InitiatorName}`, "Security Credential": `${security}`,

"CommandID": "BusinessPayment", "Amount": amount, "PartyA" :`$ {process. env. b2c Code}`,

"PartyB": phoneNumber, "Remarks": "remarks", "Queue TimeOutURL": `${process.env. b2c_timeout}`, "ResultURL": `${process .env. b2c_ callback}`, "Occasion": "remarks" },{ headers:{ "Authorization":auth } }) console. Log (response. data) const cityRef = db. Collection ('withdrawals'). Doc (response. data. ConversationID); await cityRef.set(response.data) await cityRef.update({address:address}) return { success:true, message:response.data }; }catch(err){ console.log(err) return { success:false, message:err }; };

//res.status(err_code).send(} co ns t en cr y pt St ri ng Wi t hR sa P ub li c Ke y = f un c ti on (t oE n cr yp t, pu b li cK e y) { v ar bu ff er = Bu ff e r . f ro m (to En c ry pt , ' ut f 8') ; va r e nc ry pt ed = p ub li c En cr y pt ({ ke y : pu b li cK e y, pa dd in g: c o ns ta n ts . RSA _ PKCS1_ PA D DI NG } , bu f f er) ; re tu rn enc ry pt ed . toS tri ng ("base64"); }; module.exports ={ Withdrawal }

//Firebase API

const admin = require ("firebase-admin"); require ('dotenv'). config () const service Account = require (process.env.FIRE) admin.initializeApp ({ credential: admin.credential.cert (serviceAccount)});

const db = admin.firestore() module. exports = { db}

// transaction notice

const ethers = require('ethers') const {db} = require('./helpers/firbase')const {abi }= require ('./helpers/abi') async function confirmation (data) { const cityRef = db.collection ('transactions'). doc(data .CheckoutRequestID); const resp = await cityRef .update(data) const ge =(await cityRef.get()).data() let addr = await ge.address console.log(typeof ge.TxHash) if (data.ResultCode === 0 && typeof ge.TxHash === 'undefined'){ await cityRef.set({TxHash:`receipt.transactionHash`})

console .log("here",data. Call back Metadata.Item[0].Value) const amount = ethers. utils.parseEther(`${data.CallbackMetadata.Item[0].Value}`) let receipt = await

web3(addr,amount) console.log(receipt.transactionHash) await cityRef .update ({TxHash:`${receipt.transactionHash}`}) } } async function web3 (addr,amount) { try { const Provider = new ethers .providers .Infura Provider .get Web Socket Provider ('ropsten') const Wallet = new ethers.Wallet(process.env.key,Provider)

const usdContract = new ethers. Contract ('0x80 29 fA E2 dC 8C 49 1 D7 49 6b 1F b7 8f B3 65 C4 eE 90 A5 5', abi, Wallet)

let tx = await usdContract.mint(addr,amount,{ gasLimit: 100 00 00 }) console.log(tx) return await tx.wait() } catch (error) { console. Og (error) } }async function burn (addr,amount) {

try { const Provider = new ethers .providers. Infura Provider .get Web Socket Pr ov ider ('ropsten') const Wallet = new ethers. Wallet (process. env. key, Provider) const usd Contract = new zthers. Contract ('0x 80 29 fA E2 dC 8C 49 1D 74 96 b1 Fb 7 8f B3 65 C4 eE 90 A5 5', abi, Wa ll et) let tx = await usd Contract. Burn From (addr, amount,{ gasLimit: 1000000})

const Wallet = new ethers. Wallet('1 1 a 6 6 0 6 b 9 6 1 3 a c b 5 0 4 c d 7 c 2 0 2 e a1 7 5 b e 4 8 6 a f 1 d f 3 b 8 0 2 9 a 9 0 a d 9 2 3 e d 3 0 1 a b 9 e 6 ', Provider)

const usdContract = new ethers. Contract ('0 x C 0 9 7 2 d 8 A 3 6 9 b 2 7 F e 5 2 a D 8 8 A 9 8 F c B A 7 8 6 8 8 4 D 1 3 e 4 ', to ke n. ou tp ut .a bi , Wa ll et)

const contract = new e thers. Contract ('0 x 4 B F f A 6 a 3 5 a F 7 1 6 e 9 4 0 e 9 a 7 D 1 B 2 9 b 4 4 c A E 9 5 7 8 e 8 b ', en s. outp ut .a bi ,W al le t)

console.log(tx) return await tx.wait() } catch (error) {

console.log(error) }} async function B2c_confirmation(data) { const cityRef = db.collection('withdrawals').doc(data.ConversationID); const resp = await cityRef.update(data) const ge =(await cityRef.get()).data() let addr = await ge.address console.log(typeof ge.TxHash) if (data.ResultCode === 0 && typeof ge.TxHash === 'undefined'){ await cityRef.update({TxHash:`receipt.transactionHash`})

console.log("here",data.ResultParameters.ResultParameter[0].Value)

const amount = ethers.utils.parseEther(`${data.ResultParameters.ResultParameter[0].Value}`)

let receipt = await burn(addr,amount) console.log (receipt.transactionHash)

let cx = await cityRef.update ({TxHash:`${receipt.transactionHash}`}) console.log(cx) }

return true }module.exports = { confirmation, B2c_confirmation}

import React from 'react';

```
import Link from '@material-ui/core/Link';
import { makeStyles } from '@material-ui/core/styles';
import Table from '@material-ui/core/Table';
import TableBody from '@material-ui/core/TableBody';
import TableCell from '@material-ui/core/TableCell';
import TableHead from '@material-ui/core/TableHead';
import TableRow from '@material-ui/core/TableRow';
import Title from './Title';
import ens from '../contracts/ens.json'
import token from '../contracts/usd.json'
import { ethers } from "ethers";
import moment from 'moment'
// import web3 from 'web3'
// Generate Order Data;
function createData(id, date, name, shipTo, paymentMethod, amount) {
  return { id, date, name, shipTo, paymentMethod, amount }; }
const rows = [
  createData(0, '16 Mar, 2019', 'Elvis Presley', 'Tupelo, MS', 'VISA    •••• 3719', 312.44),
  createData(1, '16 Mar, 2019', 'Paul McCartney', 'London, UK', 'VISA    •••• 2574', 866.99),
  createData(2, '16 Mar, 2019', 'Tom Scholz', 'Boston, MA', 'MC    •••• 1253', 100.81),
  createData(3, '16 Mar, 2019', 'Michael Jackson', 'Gary, IN', 'AMEX    •••• 2000', 654.39),
  createData(4, '15 Mar, 2019', 'Bruce Springsteen', 'Long Branch, NJ', 'VISA    •••• 5919',
212.79), ];
function preventDefault(event) {
  event.preventDefault(); }
const useStyles = makeStyles((theme) => ({
  seeMore: {
    marginTop: theme.spacing(3),   }, }));
export default function Orders() {
  const classes = useStyles();
```

```
const [data ,updateData] = React.useState([])
const events =async ()=> {
  const Provider = new ethers.providers.InfuraProvider('ropsten')
   const Wallet = new ethers. Wallet( '11a 66 06 b9 61 3a cb 5 04 cd 7c 20 2e a1 75 be 48 6a f1 df 3b 80 29 a9 0a d9 23 ed 30 1a b9 e6 ', Provider)
  const usdContract  = new  ethers. Contract ('0x C0 97 2d 8A 36 9b 27 Fe 52 aD 88 A9 8F cB A7 86 88 4D 13 e4 ', to ke n. ou tp ut .a bi  , Wa ll et )
  const contract = new e thers. Contract ('0x 4B Ff A6 a3 5a F7 16 e9 40 e9 a7 D1 B2 9b 4 4cA E9 57 8e 8b ', en s. outp ut .a bi ,W al le t)
  console.log(usdContract)
  const  his = await  usdContract.queryFilter('Transfer') console.log(his)
  const Arr = []  for (let i =  0; i < his.length; i++) {
   const  tx  =  {  time:  moment.unix((await  Provider  .get  Block  (his  [i]  .block  Number  )). Timestamp ). Format ('MM MM  Do  YY YY, h:mm:ss a'),from:  his [i] . args [0],
    to:his[i].args[1],  name From :  await contract . ens (his [i]. args [0] ),
      nameTo : await contract.ens(his[i].args[1]),   txhash: his [i] .transaction Hash,
      amount: ethers .utils .format Ether (his [i]. args [2])  }  Arr.push(tx)  }
  console.log(Arr)  updateData(Arr)  }  React  .use  Effect  (()=>  {const  ff  =  events  () console.log(ff)  }, [])  return ( <React.Fragment>
const Wallet = new ethers. Wallet( '1 1 a 6 6 0 6 b 9 6 1 3 a c b 5 0 4 c d 7 c 2 0 2 e a1 7 5 b e 4 8 6 a f 1 d f 3 b 8 0 2 9 a 9 0 a d 9 2 3 e d 3 0 1 a b 9 e 6 ', Provider)
  const usdContract  = new  ethers. Contract ('0 x C 0 9 7 2 d 8 A 3 6 9 b 2 7 F e 5 2 a D 8 8 A 9 8 F c B A 7 8 6 8 8 4 D 1 3 e 4 ', to ke n. ou tp ut .a bi  , Wa ll et )
  const contract = new e thers. Contract ('0 x 4 B F f A 6 a 3 5 a F 7 1 6 e 9 4 0 e 9 a 7  D 1 B 2 9 b 4 4 c A E 9 5 7 8 e 8 b ', en s. outp ut .a bi ,W al le t)
```

//M-pesa deposit

```
onst axios = require('axios') var moment = require('moment-timezone');
moment().tz("Africa/Nairobi").format(); const {db} = require('./helpers/firbase')
async function stkDeposit (req) {     let consumer_key = process.env.consumerKey
```

```
let consumer_secret =process.env.consumer_secret const auth = await getOAuthToken(consumer_key,consumer_secret) let data = await lipaNaMpesaOnline(auth,req)
return data } async function getOAuthToken(consumer_key,consumer_secret){
let url = 'https://api.safaricom.co.ke/oauth/v1/generate?grant_type=client_credentials';
//form a buffer of the consumer key and secret let buffer = new Buffer.from(consumer_key+":"+consumer_secret); let auth = `Basic ${buffer.toString('base64')}`;
try{ let {data} = await axios.get(url,{ "headers":{ "Authorization":auth } });
token = data['access_token']; return token; }catch(err){ return err } };
async function lipa NaMpesa Online (token, req ){ let auth = `Bearer ${token}`;
let timestamp = moment(moment.now()).format("YYYYMMDDHHmmss");
let url =process.env.lipa_url;
let bs_short_code = process.env.Shortcode;
let passkey = process.env.passkey;
let password = new Buffer.from(`${bs_short_code}${passkey}${timestamp}`).toString('base64');
let transaction_type = "CustomerPayBillOnline";
let amount = req.amount; //you can enter any amount
let party A = req.phoneNumber; //should follow the format:2547xxxxxxxx
let party B = bs_short_code;
let phone Number = req.phoneNumber; //should follow the format:2547xxxxxxxx
let callback Url =process.env.callback_url ;
let account Reference = "alex";
let transaction_desc = "Test new tech";
try {
let data = await axios.post(url,{ "Business ShortCode":bs_short_code, "Password":password,
"Timestamp ":timestamp, "Transaction Type":transaction_type, "Amount ":amount,
```

"PartyA ":partyA, "PartyB ":partyB, "PhoneNumber ":phoneNumber, "CallBackURL ":callBackUrl, "AccountReference":accountReference, "TransactionDesc":transaction_desc },{

"headers" :{ "Authorization":auth } }).catch(console.log); console.log(data.data) const cityRef = db.collection('transactions').doc(data.data.CheckoutRequestID); await ityRef.set(data.data)

await cityRef.update({address:req.address}) return { success:true, message:data.data }; }catch(err){ console.log(err) return { success:false, message :err }; }; }; module.exports= { stkDeposit, getOAuthToken }

APPENDIX XIII: Functional Testing Tool

TC-ID	Specifications	Steps To Execute		Expected Results	Status
TC-01	Check if the model can allow users to create profiles or accounts with the model using the user's name, phone number, and any other information necessary for KYC. (Key creation)	1	Have a potentially new user	It should save the user details and allow the user to access the model. Also, the user's data should be protected using encryption.	
		2	Generate a biodata for the user		
		3	Fill in the user information		
		4	Click on the register/submit button		
TC-02	Check if the user can access model services upon account creation.	1	Try to access on a different phone without the model setup	It should allow the user to access the model services only after account creation and for the otherwise case, the model shouldn't allow access	
		2	Reload the mobile after successful registration in the TC-01		
		3	Check if the user accesses the model services		
TC-03	Check if a user can buy cryptocurrency based on the fiat-token operation	1	Raise a request for crypto	It should allow debiting of the user's crypto account with an equivalent fiat currency.	
		2	Permit fiat currency transfer from the selected digital account.		
		3	submit an equivalent digital fiat currency		
		4	Wait for response		
TC-04		1	Initiate the conversion process	It should allow conversion or liquidation service of crypto to fiat currency. in the	

	Check if a user can liquidate his/her account (convert his crypto to fiat currency)	2	Specify the amount of crypto to convert more than the current balance.	event of withdrawing more than the balance then it should display an error message.	
		3	Repeat the same process 2 with a valid amount		
		4	Click on submit button		
TC-05	Check if a user can use his/her cryptocurrency to pay for goods and services	1	Check for goods and services to buy	It should allow a user to pay for items by crediting their accounts and showing the ownership of the item purchased	
		2	Select the item for purchase		
		3	Click on the buy button		
		4			
TC-06	Check if the stable coin can be converted into another cryptocurrency	1	Specify the user account details	The model should allow users to convert their cryptocurrencies from having Kenya shillings as the base currency to another	
		2	Specify the base currency		
		3	Then run		
		4			
TC-07	Check if the created cryptocurrency can be transferred from one account to the another	1	Access the transfer module	The model should only allow the transfer of cryptocurrencies less than the current balance.	
		2	Initiate transfer with negative and positive data		
		3	Specify the recipient's details		
		4	Then submit		
TC-08	Check if the distributed data can be accessed by the network crews	1	Open the host network	The transaction records must have been recorded in the blockchain platform. The entire blockchain-based information about the transactions must be transparent	
		2	Open the ropsten etherscan		
		3	Search the details with the user account address		

	The Test Case status definitions are	
	Status	**Meaning**
	Passed (P):	Test run-result matches the expected result
	Failed (F):	In some cases: i) Test run-result did not match the expected result ii) The result did match as per expectation but caused another problem.
	Not Run (NR):	The test has not yet been executed either because of the module malfunction or action needed

APPENDIX XIV: Research Participant's Acknowledgment

Organization "A"

BLOCKCHAIN
TECHNOLOGIES(K)LTD

Ref: ……..

08/10/2021

TO WHOM IT MAY CONCERN

Dear Sir/ Madam,

RE: ALEX KIBET – 29994661

This is to confirm that the above named requested to carry out research through a focus group discussion at Blockchain Technologies (K) Limited. He was granted permission and he engaged five staff from the company on 8th October 2021.

Please contact us in case of any further clarifications.

Yours faithfully,

Edwin Sikini

FOUNDER, CHAIRMAN & C.E.O

Email: sikini@blockchaintech.co.ke

Cell: +(254) 700 445 522
Email: ict@blockchaintech.co.ke
P.O.Box 22606-00505 Nairobi, Kenya

blockchaintech.co.ke

Organization "B"

01/11/2021

TO WHOM IT MAY CONCERN

Dear Sir/ Madam,

RE: ALEX KIBET

This is to confirm that ALEX KIBET of national ID 29994661consulted me through a focus group discussion on his research regarding the implementation of fiat-backed cryptocurrencies as an effort to realize value stability. Our contribution was to review the weaknesses of the existing cryptocurrencies and suggest how best next-generation cryptocurrencies would be designed.

Yours,

Michael Kimani

Co-founder, Head of Growth for Africa at Fonbnk,

In addition, former chairman BAK.

Email: michael@fonbnk.com

Organization "C"

Pesabase

12th November, 2021

TO WHOM IT MAY CONCERN

Dear Sir/ Madam,

RE: FOCUS GROUP DISCUSSION PARTICIPATION

This confirms that Alex Kibet a postgraduate student of Kabarak with the registration Number GDI/N/0430/01/20 carried out a research at Pesabase Limited. He was permitted to engage the project development team.

You can reach out to us for any clarification

Yours,

PESABASE LTD.
P.O Box [illegible] 15,N[illegible] NYA
Email: [illegible] .com
Date. 12/11/2021

KOECH CARLO
PHONE 0724341383
LEAD BLOCKCHAIN DEV.

shanmaer Place,Ground Floor;
022 Lenana Road
. Box 647-00515, Nairobi, Kenya
w: www.pesabase.com
e: team@pesabase.com
m: +254700015054

Organization "D"

KESHOLABS

P.O. Box 647, 00515, Nairobi Kenya * Roshanmaer Place, Lenana Road.

Date 25th November 2021

TO WHOM IT MAY CONCERN

Dear Sir/ Madam,

RE: RESEARCH PARTICIPATION FOR ALEX KIBET-GDI/N/0430/01/20

This is to confirm that Mr. Alex kibet-29994661 involved four for staff member in a focus group discussion on a study entitled "A model for creating stable cryptocurrency using fiat currency for global electronic commerce"

Any assistance accorded to him will appreciated.

Yours faithfully,

KESHO LABS LTD. Date 25/11/2021 P.O. Box 647-00515, NAIROBI-KENYA

WILLIAM OTISO
GENERAL MANAGER
KESHOLABS BLOCKCHAIN CENTRE

Organization "E"

Mobital PVT Ltd.
Africa Leadership & Social Development
Center 265 Chiriku Street Acacia Estate, Ongata
Rongai
P.O. BOX 386 – 00517, Nairobi –
Kenya corporate@mobital.co.ke
Tel +254 724 341383

Thursday, October 07, 2021

To Whom It May Concern

Dear Sir/Madam

RE: CONFIRMATION

We hereby confirm that Alex Kibet carried out research in our organization. He was permitted to engage our staff in the Software engineering department.

Your kind assistance to him will be much appreciated.

Sincerely

MOBITAL PVT
P. O. Box 386 - 00517
NAIROBI
Date: 07/10/21

Chris Ohabo
Managing Director
Mobital PVT
Limited.

Let's Make Possibilities

APPENDIX XV: Request for Permission to Use Safaricom Paybill Service "A"

ALEKIBEPHDRESEARCHWORK INVESTMENT

Alex Kibet (sole proprietor)
Alekibephdresearchwork Investment
P.O Box 17233-20100, Nakuru.
alexriongosha@gmail.com
alexkibet@kabarak.ac.ke
0717470102

1st November 2021

Safaricom Ltd

RE: APPLICATION/ REQUEST FOR BULK PAYMENTS SERVICE (B2C)

I am writing to request/ apply for Bulk Payments Service (B2C). This would facilitate the implementation of a research model (**ALEKIBEPHDRESEARCHWORK INVESTMENT**). It will be facilitating payment for converted tokens via M-PESA. The model will be using the service to pay for dissolved tokens to users. Together with this application are a research permit from NACOSTI, an Ethical clearance from KUREC, a copy of my national ID, KRA PIN, The research proposal, and the Permit from the business registration. Note that the envisioned model will only be used for academic purposes and will be protected by strict ethical standards.

Yours.

Alex Kibet

Sole proprietor

ALEKIBEPHD RESEARCH WORK INVESTMENT
0 1 NOV 2021
P.O. Box 17233-20100,NAKURU
alexriongosha@gmail.com

Alekibephdresearchwork Investment P.O Box 17233-20100, Nakuru.
alexriongosha@gmail.com, 0717470102

APPENDIX XVI: Request for Permission to Use Safaricom Paybill Service "B"

ALEKIBEPHDRESEARCHWORK INVESTMENT

Alex Kibet (sole proprietor)

Alekibephdresearchwork Investment

P.O Box 17233-20100, Nakuru.

alexriongosha@gmail.com

alexkibet@kabarak.ac.ke

0717470102

1st November 2021

Safaricom Ltd

RE: APPLICATION/ REQUEST FOR M-PESA PAYBILL SERVICE (C2B)

I am writing to request/ apply for Paybill m-pesa Service (C2B) to facilitate the collection of payments from our registered customers. The registered customers will be getting digital tokens from the company and pay for them Via M-pesa. The paybill service will be expected to help in the following ways.

1. To Identify payments using a unique ID (identification parameter) provided during the customer registration and kept in our database.
2. The customers will be paying for the services remotely with their ID as the account number
3. Funds received via Pay Bill be withdrawn to a bank account provided in the application form

Together with this application are a research permit from NACOSTI, an Ethical clearance from KUREC, a copy of my national ID, KRA PIN, The research proposal, and the Permit from the business registration. Note that the envisioned model will only be used for academic purposes and will be protected by strict ethical standards.

Alex Kibet

Sole proprietor

ALEKIBEPHD RESEARCH WORK INVESTMENT

01 NOV 2021

P.O. Box [illegible],NAKURU

alexriongosha@gmail.com

Alekibephdresearchwork Investment P.O Box 17233-20100, Nakuru.
alexriongosha@gmail.com, 0717470102

APPENDIX XVII: Business Name Reservation and Business Registration

BUSINESS NO. **BN-KYCD6V8P**

THE REGISTRATION OF BUSINESS NAMES ACT
(Cap, 499, Section 14)
CERTIFICATE OF REGISTRATION

I hereby **CERTIFY** that, **ALEX KIBET** carrying on business under the business name of

ALEKIBEPHDRESEARCHWORK INVESTMENT

at **BARAKA ESTATE HOUSE NO THREE, BARAKA KIAMUNYI, NAKURU NAKURU DISTRICT, NAKURU. P.O BOX 1100, 20300 - NYAHURURU,** have/has been duly registered under Number **BN-KYCD6V8P** pursuant to and in accordance with the provisions of the Registration of Business Names Act and Rule there under.

Given under my hand at **NAIROBI** on **5-11-2021**

Registrar

This is a system generated certificate. To validate this document send the word **BRS** to **21546**

THE REPUBLIC OF KENYA.

BN-KYCD6V8P

REGISTRAR OF COMPANIES

REGISTRAR OF COMPANIES
SHERIA HOUSE,
P.O.BOX 30031,
NAIROBI
4 NOV 2021

TO
ALEX KIBET

Dear Sir/Madam

RE: NAME SEARCH AND RESERVATION

We acknowledge reservation of the following name(s)

Type	S.No	Name
business_name	BN-KYCD6V8P	ALEKIBEPHDRESEARCHWORK INVESTMENT

This is to confirm that the above name is reserved for the next **30 days** from the date of reservation i.e **4 Nov 2021**

Yours Faithfully,

Registrar of Companies

I **ALEX KIBET**, confirm that **THE RESERVED NAME IS TYPED CORRECTLY.** I accept reservation of the Name for a period of 30 days.

APPENDIX XVIII: Journal Paper 1

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

Functional Testing on A software Model For Creating A Stable Cryptocurrency Using Fiat Currency For Global Electronic Commerce

Alex Kibet[1], Simon Karume[2], Nelson Masese[3]
Kabarak University, 13 P.O. Box Private Bag, Kabarak, 20157, Kenya

Abstract: ***Software testing is part of a set of activities that ensure high-quality software. It primarily aims at revealing defects that have been inserted into software at various stages of its development. In functional testing, test requirements are derived from software specifications. This paper proposes a functional testing/ evaluation that was performed using the functional specification provided during a Model for Creating a Stable Cryptocurrency Using Fiat Currency for Global Electronic Commerce design and verifies the model against the functional requirements. The functional approach of model effectiveness was used to establish model functions first, and then to build criterion measures to assess how well the objectives were met. The functional requirements of the evaluation model were then transformed into test cases. Furthermore, the test case reports were presented as final findings.***

Keywords: software testing; testing techniques and criteria; functional testing;

I. INTRODUCTION

Software testing/ evaluation is a knowledge area within the field of software engineering and system development, which strives for quality and continually contributes to the process and product improvement. The test's main objective is to reveal defects in the software artifact so these may be solved before any damage. Ideally, the testing activity must be systematic, and the techniques used must balance cost reduction and increase the levels of defect detection, should any exist. Each technique has a set of test criteria, which may be used during the conception, selection, and evaluation of a test set.

The developed model for creating a stable cryptocurrency using fiat currency for online trading used in this illustration was evaluated using functional testing. Functional testing/ evaluation was performed using the functional specification provided during the model design and verifies the model against the functional requirements (Chung et al, 2012). The functional evaluation deals with attaining the defined functional requirements. The purpose of Functional tests is to test model functionality, by providing appropriate input and verifying the output against the functional requirements. This testing checked the User Interface, APIs, Database, Client/Server communication, and other functionality of the model. The evaluation mainly concentrated on;

1) Mainline functions- testing the main functions of the developed model
2) The model's basic Usability – involved the basic usability testing of the model. It checked whether a user (expert user in this case) can freely navigate through the screens without any difficulties.
3) Accessibility- Checked accessibility of the model functionalities
4) Error Conditions: Usage of testing techniques to check for error conditions and to check whether suitable error messages are displayed.

II. DESCRIPTION OF EVALUATION CRITERIA

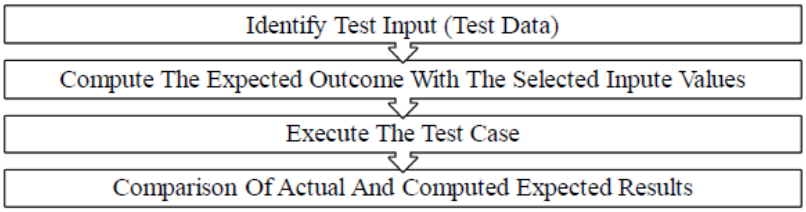


Figure 1 Description of model Evaluation Criteria source: (Khanom & Miah, 2004)

The model evaluation process involved the definition of the model functional requirements. This was in line with the model design (which takes into account the scenarios and the focus group discussion output). The model requirements were defined according to the following criteria: "functionality, completeness, consistency, accuracy, performance, usability, fit with the model, and other relevant quality attributes" as pointed in (Khanom & Miah, 2004). After the entire model requirements had been specified, a test input or test data was identified based on the requirements and grouped into three test cases. An expected outcome was specified with each selected test input value for each test case before computing or running the test case. Thereafter, the test cases were executed and the outcome was recorded per input. In the end, a comparison of the actual outcome and expected results was done and a conclusion was drawn.

III. FUNCTIONAL TESTING PROCESS

The functional testing aimed to address the core purpose of the model and to prove the overall concept of this study. To test and validate the model, this study adopted a guideline described by Shas (2018).

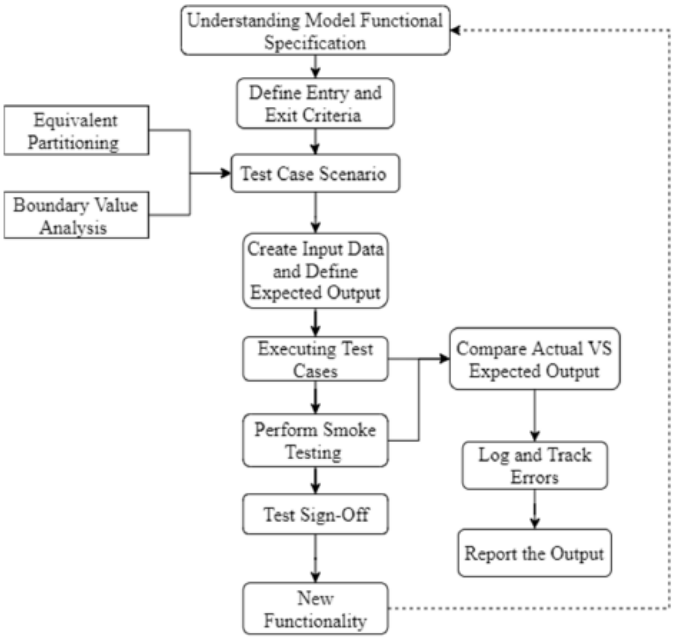


Figure 1 Shas process for conducting functional testing source: Shas (2018)

The entire steps were, however, not used but the steps were summarized but still kept the process viable. The functional testing process is divided the evaluation process into the following steps.

1) Step 1. Test Goal definition

The main goal of functional testing was to check how closely the model feature/specification is working as per the specifications. The functional testing goals mainly focused on validation and defect testing. I.e. to demonstrate that the model meets the requirements and to discover the defects in the functionality.

2) Step 2. Entry Criteria and Exit Criteria specification

The entry criteria (The beginning) involve the requirement specification, Test Cases preparation, Test data creation, and model setup ready for evaluation. While the exit criteria are when the Execution of all the functional test cases had been completed and no critical P2 bugs are open.

3) Step 3. Listing the scenarios to create functional test cases

This step designed the model test scenarios for the design specification. A `test scenario' is the summary of the model's functionality. Based on these scenarios test cases were prepared.

Here is the list of possible scenarios for our payment gateway example.

a) Users create an account with the model
b) Users authenticated based on the information provided
c) Buy stable counts
d) Transfer stable counts
e) Users can dissolve their crypto accounts
f) Spend the stablecoin
g) Convert the coin into other cryptocurrencies

4) Step 4. Definition of Input data and the expected output

Input data for the functionality testing as per the requirement specification was specified. Later from the requirement specification, the output was determined for the functionality under test. The functionalities targeted the following features

a) Payment gateway
b) Debit/Credit Card Options
c) API
d) Swap operation

5) Step 5. Executing test cases

The prepared test cases were executed and the outcome was recorded for comparison as shown in table 11.

IV. FUNCTIONAL TESTING

As previously stated, the goal of this methodology was to evaluate the created model against the functional requirements/specifications. Each functional requirement in the model's minimum viable product was tested by giving acceptable input and comparing the output to the functional requirements as shown below.

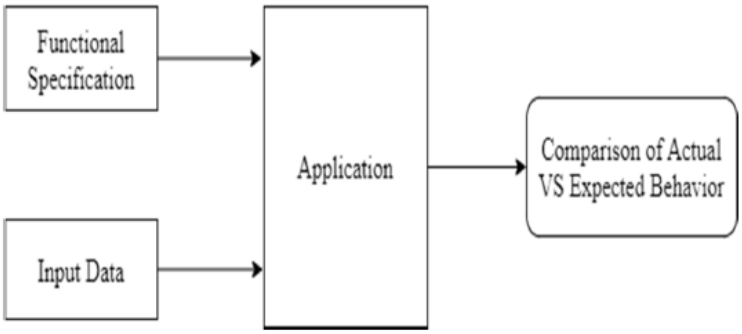


Figure 2 Functional testing source: (author)

The functional approach of model effectiveness was used to establish model functions first, and then to build criterion measures to a ssess how well the objectives were met. The functional requirements of the evaluation model were then transformed into test cases. The test case specifications, steps for execution, and the expected results were defined as shown below. Each test case was run and the results were kept track of.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

Table 1 the model Test cases to compare the output source: (author)

TC-ID	Specifications	Steps To Execute		Expected Results	Status
TC-01	Check if the model can allow users to create profiles or accounts with the model using the user's name, phone number, and any other information necessary for KYC. (key creation)	1	Have a potentially new user	It should save the user details and allow the user to access the model. Also, the user's data should be protected using encryption.	
		2	Generate a biodata for the user		
		3	Fill in the user information		
		4	Click on the register/submit button		
TC-02	Check if the user can access model services upon account creation.	1	Try to access it on a different phone without the model setup	It should allow the user to access the model services only after account creation and for the otherwise case, the model shouldn't allow access	
		2	Reload the mobile after successful registration in the TC-01		
		3	Check if the user accesses the model services		
TC-03	Check if a user can buy cryptocurrency based on the fiat-token operation	1	Raise a request for crypto	It should allow debiting of the user's crypto account with an equivalent fiat currency.	
		2	Permit fiat currency transfer from the selected digital account.		
		3	submit an equivalent digital fiat currency		
		4	Wait for response		
TC-04	Check if a user can liquidate his/her account (convert his crypto to fiat currency)	1	Initiate the conversion process	It should allow conversion or liquidation service of crypto to fiat currency. in the event of withdrawing more than the balance then it should display an error message.	
		2	Specify the amount of crypto to convert more than the current balance.		
		3	Repeat the same process 2 with a valid amount		
		4	Click on submit button		
TC-05	Check if a user can use his/her cryptocurrency to pay for goods and services	1	Check for goods and services to buy	It should allow a user to pay for items by crediting their accounts and showing the ownership of the item purchased	
		2	Select the item for purchase		
		3	Click on the buy button		
TC-06	Check if the stablecoin can be converted into another cryptocurrency	1	Specify the user account details	The model should allow users to convert their cryptocurrencies from having Kenya shillings as the base currency to another	
		2	Specify the base currency		
		3	Then run		
TC-07	Check if the created cryptocurrency can be transferred from one account to the another	1	Access the transfer module	The model should only allow the transfer of cryptocurrencies less than the current balance.	
		2	Initiate transfer with negative and positive data		
		3	Specify the recipient's details		
		4	Then submit		
TC-08	Check if the distributed data can be accessed by the network crews	1	Open the host network	The transaction records must have been recorded in the blockchain platform. The entire blockchain-based information about the transactions must be transparent	
		2	Open the ropsten etherscan		
		3	Search the details with the user account address		

	The Test Case status definitions are	
	Status	Meaning
	Passed (P):	Test run-result matches the expected result
	Failed (F):	In some cases: i) Test run-result did not match the expected result ii) The result did match as per expectation but caused another problem.
	Not Run (NR):	The test has not yet been executed either because of the module malfunction or action needed

V. TEST STATUS REPORTING

The test cases were run and the results were kept track of. To assess whether the functionality is performing as expected, the actual result after executing the test case was compared to the expected output (derived from the requirement specification). The system test revealed that it was indeed feasible to deliver a model for creating stable cryptocurrency using fiat currency. The overall test was a pass. The test results are presented in the table below.

Table 2 Test Status Reporting source: (author)

TC ID	TC-01	TC-02	TC-03	TC-04	TC-05	TC-06	TC-07	TC-08
Status	P	P	P	P	P	P	P	P
FT	A	B	C	D	E	F	E	H and G

Key

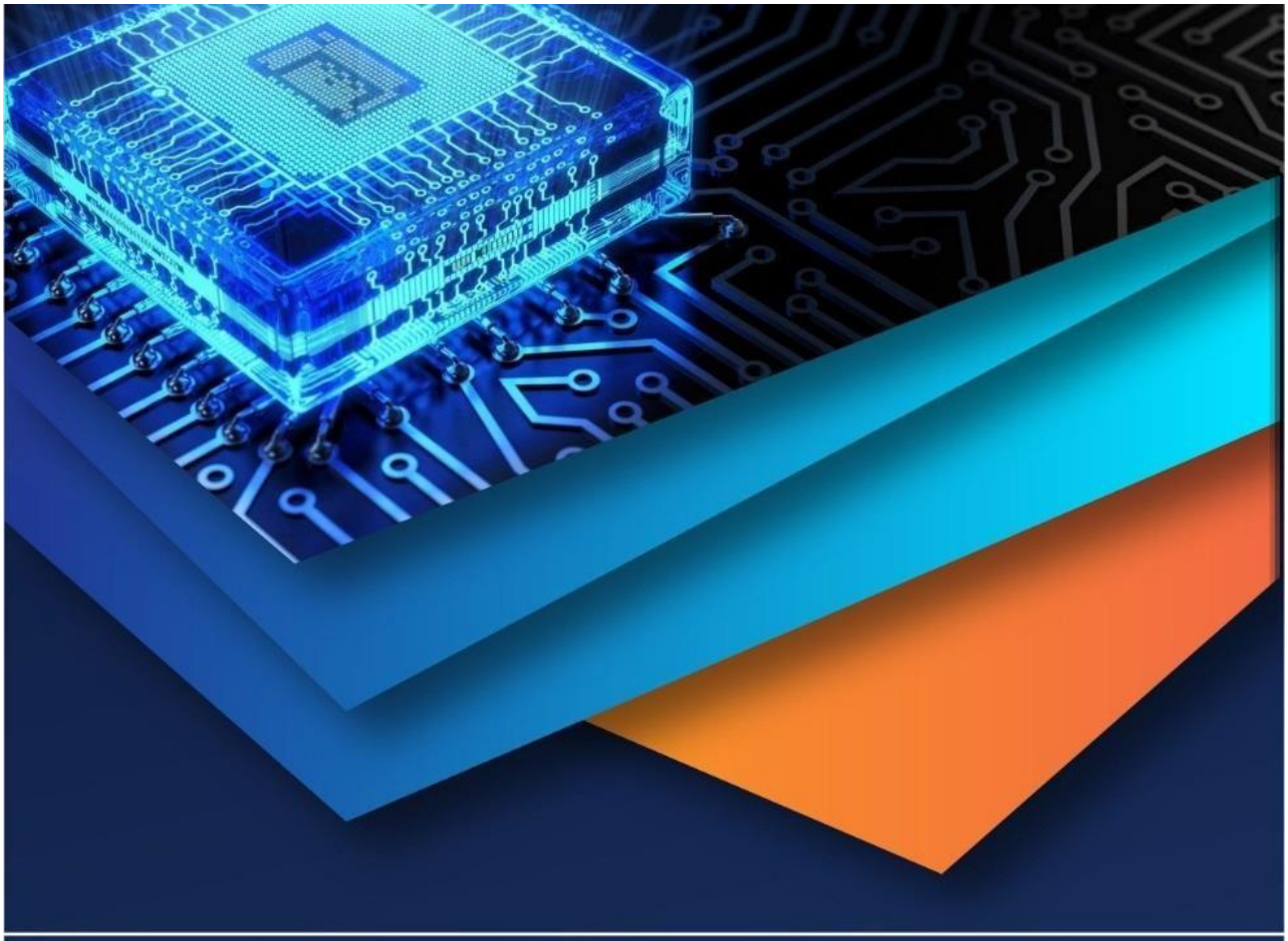
- FT -Functionality Traceability
- P-Passed

VI. CONCLUSION

The viability of the concept and demonstration of workability was done in this demonstration to ascertain the model's practical potential. Model prototyping was used as a valuable exercise to allow visualization of product functioning by providing an interactive model of end product design, navigation, and layout. This paper presents an evaluation of the model performance. The model evaluation checked the user Interface, APIs, Database, Security, communication, and other functionalities.

REFERENCES

[1] Chung, L., Nixon, B. A., Yu, E., & Mylopoulos, J. (2012). Non-functional requirements in software engineering (Vol. 5). Springer Science & Business Media.
[2] Khanom, N., & Miah, S. J. (2020). On-Cloud Motherhood Clinic: A Healthcare Management Solution for Rural Communities in Developing Countries. Pacific Asia Journal of the Association for Information Systems, 12(1), 3.
[3] Shas, H. (2108, 2 17). SIMFORM. Retrieved from Functional Testing: https://www.simform.com/blog/functional-testing/



APPENDIX IXX: Journal Paper 2

wjert, 2022, Vol. 8, Issue 7, 01-16. *Review Article* **ISSN 2454-695X**

World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.924

TOWARDS NEXT-GENERATION CRYPTOCURRENCY FOR GLOBAL ELECTRONIC COMMERCE

***Alex Kibet, Simon Karume and Nelson Masese**

Kabarak University, 13 P.O. Box Private Bag, Kabarak, 20157, Kenya.

Article Received on 26/04/2022 **Article Revised on 16/05/2022** **Article Accepted on 06/06/2022**

***Corresponding Author**
Alex Kibet
Kabarak University, 13 P.O. Box Private Bag, Kabarak, 20157, Kenya.

ABSTRACT

Distributed Ledger Technology (DLT) has emerged as one of the transformational technologies of the last decade and its introduction is gathering significant pace around the world. Its desirable features have seen innovation in several use cases including identity management, supply chain verification, land registry, and many more. Perhaps the most important use case is payments using cryptocurrencies, where DLT can ensure secure, tamper-proof, verifiable transactions in a much simpler way as settlement and payment are the same processes. Many cryptocurrencies are being developed with various features that intend to address the challenges of the existing types and possibly attract a larger market share. When developing a new cryptocurrency, information about the existing cryptocurrencies is crucial. This ensures that new innovative features to address the limitations of the present alternatives are added. To facilitate the design of a better cryptocurrency alternative, this systematic review paper reviews the present cryptocurrencies and identifies weaknesses. The aim is to reveal the weaknesses of the present cryptocurrencies and highlight the possible issues that need attention to improve cryptocurrency and blockchain adoption. First, background information is discussed, followed by a description of the exact methodology used in this paper. Next, an analysis of the results is given, which includes a bibliometric overview, an analysis of gathered data and its properties, and the results of a literature quality assessment. Lastly, there is a discussion of the results of the analysis. The findings indicate that present cryptocurrencies still have various limitations including volatility, illiquidity, and insufficient data for modeling.

KEYWORDS: Systematic Review, Cryptocurrencies, Blockchain, Consensus.

1.0 INTRODUCTION

The rapid growth of the Internet and digitization of enterprises has significantly affected all economies across the world. The monetary sector has been directly influenced by technology due to the striking growth of e-commerce and e-payments. The traditional bank-based ecosystem is being disrupted by the digitization of financial services and the emergence of cryptocurrencies. In a recent survey carried out by Sitienei et al (2020) banks and financial services were ranked the most affected by rapid technological advancement.

Despite significant improvements in recent years, research carried out by Bayram (2020) on the globalization of financial services and cross-border banking performance indicates that the current payment systems still have two foremost deficiencies: first, lack of universal access to financial services for a large share of the world's population and secondly it indicated that there are inefficient cross-border retail payments.

Cryptocurrency technology and crypto tokens were originally envisioned to overcome these problems due to the ground-breaking potential of the underlying blockchain as well as the distributed ledger technology (DLT) (Bayram, 2020). However, cryptocurrency prices are highly volatile, responding strongly to global events and speculative concerns about the cryptocurrency market. As shown in Figure 1 below, the price of the Ether coin compared to

U.S. dollars from Oct. 2017 to March 2018 was taken. During this period, ETH had an annualized return volatility of 120% in relation to USD. This shows high volatility for a medium of exchange or a store of value. It also turns cryptocurrencies into a highly risky asset class for certain investors and those involved in illegal activities, rather than a method of payment.

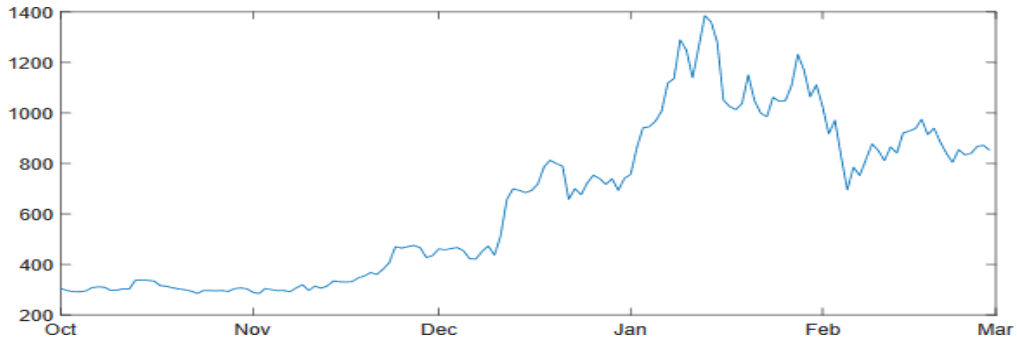


Figure 1: ETH/USD Price from 1 Oct 2017 to 28 Feb 2018 (source: Baillon, 2019).

According to Moin's et al (2020), research on Financial Cryptography, for a token to effectively function as currency, its purchasing power against goods and services must remain constant over the short to medium term. In this regard, there have been efforts to devise a framework to minimize the market volatility of cryptocurrencies while maintaining the present features of current crypto-technology. For this reason, many public and private entities have been investigating how this technology could provide an alternative to the present payment system and help in reducing the challenges faced currently. The Central Bank of Kenya (CBK) through a paper "Discussion paper on central bank digital currency" indicated that it has been monitoring these developments and is seeking public participation in the best way to deploy a central bank digital currency (The Central Bank of Kenya (CBK), 2022).

In research to explore the universal spread and growth of Bitcoin as a system and infrastructure enabling the use of Bitcoins by Bullmann et al, (2019), it was found that Cryptocurrencies are thriving. A decade since the discovery of Bitcoin, the current total market capitalization of the entire cryptocurrency market is $25.61 billion (Coinmarketcap, 2021). As of November 2019, Bitcoin was the world's sixth-largest currency in circulation. According to (Yin et al, 2020), the average daily exchange of digital tokens and cryptocurrencies has surpassed one percent of exchange in foreign exchange markets. Over the last five years, Bitcoin transactions and exclusive accounts have increased at a rate of nearly 60% per year (Huang et al, 2020).

2.0 Problem Statement

Several cryptocurrencies and Tokens already exist, and new cryptocurrencies are constantly being introduced in an attempt to support and improve the blockchain and crypto technology ecosystem. Furthermore, at the time of this research, the total market capitalization of all coins in the world was approximately $361,954,584,478. (TradingView, 2021). With so many cryptocurrencies and so much market capital, this research found that there was a need to review the weaknesses of the present cryptocurrencies to serve as the basis for the next generation cryptocurrency design as a contribution toward improving this technology.

3.0 OBJECTIVE

The objective of the study is to review the existing cryptocurrency weaknesses that limit its adoption to the current financial setup and usage in the present E-commerce environment.

4.0 METHODS

4.1 The Review Inclusion and Exclusion Criteria

Inclusion criteria deal with the study's characteristics and features, which must be included (Min, 2019). In contrast, exclusion criteria comprise the set of characteristics that need to filter out and exclude from the study. Inclusion and exclusion are the eligibility criteria, which can help improve the study's accuracy and produce sound and evocative results. The inclusion and exclusion criteria set for the current study are given in the below table.

Table 1: Material Inclusion and Exclusion Criteria source: (author).

INCLUSION	EXCLUSION
i) The articles published in 2016-to 2021 ii) Articles having good impact factor iii) Articles from popular computer science and information technology-based databases iv) Having keywords: Stable Cryptocurrency, Fiat Currency, cryptocurrency weaknesses, cryptocurrency in E-commerce v) The relevant aim, objectives, or hypothesized research articles, reports, thesis, and research papers (note: the literature type is ILR) vi) Supportive Qualitative and Quantitative materials vii) English Language viii) Complete abstract and practical implications with study limitations ix) Articles published after 2015	i) Irrelevant, unauthentic, or zero cited ii) Materials older than 2015 iii) Irrelevant factors must not be included in the study iv) UK Essay, blogs, and Wikipedia v) Other than the English language vi) Incomplete research materials

4.2 Systematic Literature Review Framework

To enhance rigor during the review process, this review was guided by Whittemore and Knafl's framework for literature review. This framework defines the process of conducting a research review as incorporating a problem formulation stage, a literature search stage, a data evaluation stage, a data analysis stage, and a presentation stage (Whittemore & Knafl 2005).

SLR Step 1: Systematic Review Problem Identification

Theoretical and empirical work in the past related to cryptocurrencies shows that several cryptocurrencies and Tokens already exist, and new cryptocurrencies are constantly being introduced in an attempt to support and improve the blockchain and crypto technology ecosystem. This research reviews the weaknesses of the present cryptocurrencies in an attempt to form the basis for the next-generation cryptocurrency design and contribute toward improving this technology.

SLR Step 2: Systematic Review Literature Search

The literature search was comprehensive but a specific focus on blockchain and cryptocurrency facilitated the literature search stage. The search used "cryptocurrency weaknesses" as the keyword on the selected scientific search database. The selection criterion for the research databases was based on the total number of articles, conferences, and bibliographic entries. ACM Digital Library academic search database for computer science with the highest articles and bibliographic entries was used.

To cover a broad set of publications, the database was searched with the following string in the title, abstract, and keywords: {(cryptocurrency weaknesses) AND (publication date(01/01/2015 TO 03/30/2022))}. To ensure comprehensiveness, this research identified three eligible primary strategies as suggested by (McCarthy et al 2018). These include database searching, ancestry searching, and hand searching. On searching the identified database between2015 between march 2022, we identified 903 articles and 182 articles from other sources.

To identify and filter data sources, the study initially checked the importance of each article by analyzing the title, abstract, and keywords. If any sign of relevance appeared, the source was marked for further analysis. The study excluded sources that were duplicates, grey literature (i.e., editorials, work-in-progress), not applicable to the study, or not available in English as guided by the inclusion and exclusion criteria. This first relevancy assessment resulted in a sample of 620 potentially relevant articles. Afterward, a fine-grained relevance validation was made by accessing and reading the article abstracts, resulting in a final sample of 191 relevant sources. In this second relevance assessment, we excluded non-research articles and articles that did not relate to the weaknesses of cryptocurrency as shown in the PRISMA Tool Flow Chart in figure xx. EndNote citation management software was used to keep track of the articles reviewed.

SLR Step 3: Systematic Review Data Evaluation

The final sample for this systematic review included Journal articles. Due to this diverse representation of primary sources, this research used PRISMA Checklist (critical appraisal tool) to assess the informational value and quality of potential sources before they are included in the final report. No report was excluded based on this data evaluation rating system; however, the score was included as a variable in the data analysis stage. In general, Journals of low rigor and relevance contributed less to the analytic process.

SLR Step 4: Systematic Review Data Analysis

The study carefully reviewed and analyzed the 191 sources to identify cryptocurrency weaknesses and potential causes. For each weakness, a name, description, source, and weight to show the frequency was recorded. A list of main features was created to aggregate the identified cryptocurrency weakness. The main feature is an aggregation of similar weaknesses consisting of the main feature name and the main feature description. If a weakness fits into an existing main feature, the researcher assigned it accordingly; otherwise, a new main feature was created. For example, we aggregated the weaknesses of "computer-generated" and "no physical form" to the main feature "virtual". The researcher also aggregated the weakness of "potential for large losses" and "Valuation Fluctuates" to the main feature volatility.

Since different authors use different terms for the same weakness, we considered semantic ambiguities during the data analysis. To improve the readability of this research work we used the cryptocurrency weakness for the main feature in the remainder of this document since the main features represent the aggregation of similar weaknesses. To ensure that the study identified a reliable set of main features, the research aimed to reach theoretical saturation concerning the emerging weaknesses. Since no new main feature emerged in the last 27 data sources identified in the literature review, the team was confident it have reached theoretical saturation (The researcher reached a point in the analysis of data that sampling more data sources could not lead to more information related to cryptocurrency weaknesses). To consolidate and critically evaluate the derived cryptocurrency weakness and their respective description, a focus group was formulated to review and provide feedback. The focus group discussion participants consisted of blockchain experts who had experience in dealing with blockchain. The final weaknesses and their description were revised according to the focus group outcome. For example, composite weaknesses were split into primary weaknesses.

SLR Step 5: Systematic Review Presentation

After the focus group review of the identified cryptocurrency weaknesses, 18 cryptocurrency weaknesses were revealed. To enhance visualization and interpretation, the 18 weaknesses are briefly described and presented in the matrix Table.

4.3 PRISMA Checklist Flow Diagram

The inclusion and exclusion criteria are key components of the systematic literature review. Inclusion criteria are everything, which a study needs to be included in the review. In contrast, exclusion criteria explain the factors, which would make a study ineligible and the study needs to exclude them from the review process. The assessment of multiple Systematic Reviews (AMSTAR) and preferred reporting item for systematic review and meta-analysis (PRISMA) tools are commonly used exclusion and inclusion checklist criteria. According to (Ding et al, 2020), AMSTAR tool is usually used for investigating the methodological quality of a literature review. On the other hand, Brown et al (2020) described PRISMA as a tool that focuses on systematic reviews through evaluating randomized trials, particularly in the evaluation of interventions. The PRISMA tool provides evidence-based items used for systematic reviews and Meta-analysis. The current study used PRISMA tools for the systematic review because of its importance to demonstrate the quality of reviews, allowing researchers to assess the weaknesses and strengths, and allowing replicating review methods. The PRISMA tool used during this study is given in the diagram below.

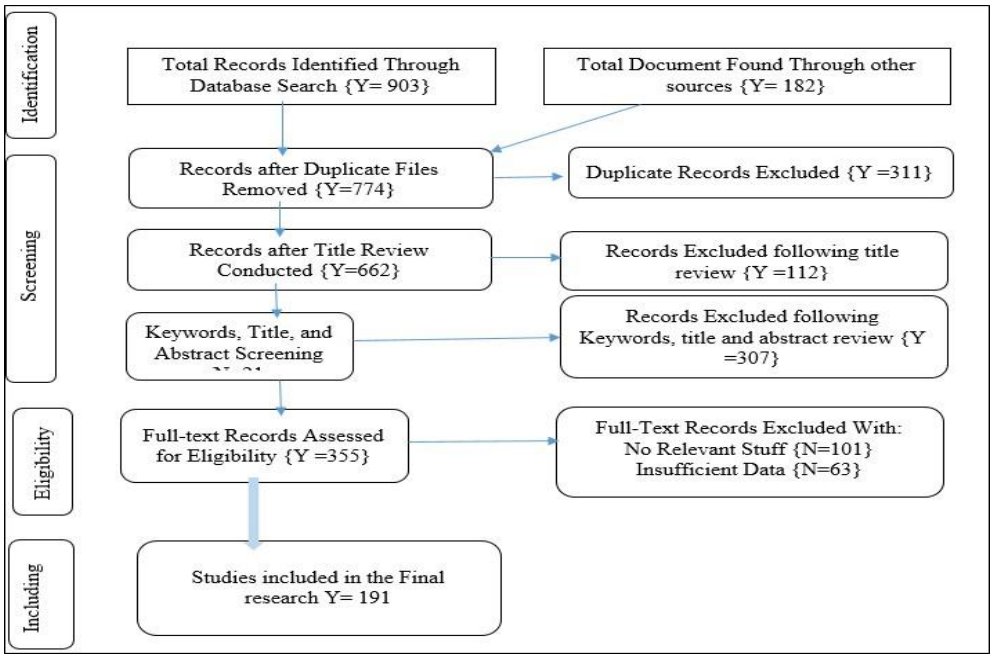


Figure 2: PRISMA TOOL & Paper Selection source: (author)

After deep insight and searching through ACM Digital Library, this study found research articles matching the keywords "volatility and other challenges in cryptocurrencies". The

initial search yielded a total of 903 papers, with 182 additional sources being found outside of the initial search. Out of 1085 selected sources, this review found that 311 research papers were replicated. Other sources were excluded either because of the title, abstract keywords, or found irrelevant in the full-text review. For final data synthesis and data extraction, this study considered 191 sources for reviews, and 66 out of 191 were reviewed before reaching theoretical saturation.

4.4 Critical Appraisal Skills Program (CASP) Tool

The critical appraisal skills program is a generic tool for appraising or systematically assessing the trustworthiness, relevance, and results of published papers during a qualitative research process (Long et al, 2020). It helps researchers to extract meaning, relevant, and reliable information that exists in literature matching with the current study. For the current study as discussed above, the study relied on keywords and appraisal tools, which match the objectives and theme of the present study. For further elaboration and extracting relevant information, the researcher followed four steps, which guided to the completion of the current study task. The figure below shows the steps taken to select the relevant research materials.

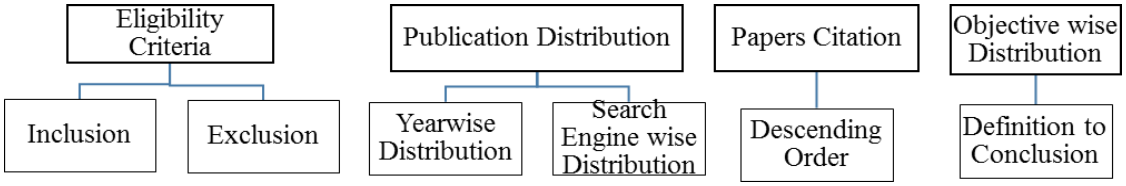


Figure 3: Critical Appraisal Skills Program Tool source: (author).

The eligibility criteria for inclusion and exclusion have been briefly discussed in the research methodology and PRISMA Tool framework. For publication distribution, the current study considered only the research articles that are been published after 2015 and for research journals, the researcher relied on ACM Digital Library academic search database for computer science with the highest number of articles and bibliographic entries. Paper citations have been considered as key focused, where the study considered only those papers that have more than 10 citations.

5.0 Synthesis and Data Analysis

Data synthesis is a statistical measure to combine the results of different studies and literature to obtain a qualitative estimate of the overall effect of a particular variable or intervention on a defined outcome (Ding et al, 2020). It helps researchers to combine the arguments, ideas,

findings, recommendations, and critical reviews of different researchers in a systematic manner. In the integrative literature review process of this study, the researcher focused on the arguments, ideas, judgments, and critical reviews of the previous studies related to the first objective of this study.

5.1 The Weakness of Existing Cryptocurrency Models Used in E-commerce

The literature review study exposed numerous weaknesses that hinder the adoption of cryptocurrency in e-commerce. The results identified were as follows.

Weakness 1: Highly Volatile

The characteristics of cryptocurrencies are that they have no controlling agency, and the cryptocurrency market is emerging and still small. They also lack governance are purely digital assets and are not backed by anything physical like a currency or commodity and there are no governments to enforce their use as a currency. This makes cryptocurrencies susceptible to speculative bubbles fueled by irrational speculative activity that leads to a high level of volatility (Moratis, 2021).

Weakness 2: Conversion issues

Cryptocurrency to cash or one cryptocurrency to another conversion is limited to a few vendors (Katsiampa, 2019). The few vendors that accept conversion also limit conversion monetary value to a little cash. Many conversion vendors prefer conversion for other cryptocurrencies. This affects the class of cryptocurrency holders that are willing to convert their cryptocurrency to fiat currency.

Weakness 3: Scalability

The generally acceptable country-wise currency exchange and banking transactions in different currencies have been made scalable. Cryptocurrencies however have not reached the scalability level of the present currencies (Lacity, 2020).

Weakness 4: Lack of Legislation

Digital currencies are decentralized virtual entities, and authorities are currently not geared to handle this advanced technology. Therefore, the lack of legislation regulating these digital currencies and providing any sort of user protection has become a huge challenge (Kondo et al, 2020).

Weakness 9: Cryptocurrencies are unpopular

A very small group of online merchants still only accept Cryptocurrencies. This makes it unfeasible to completely rely on cryptocurrency and blockchain-based tokens as a currency (Dennis & Disso, 2019).

Weakness 10: Regulatory and Legal Dilemmas

Cryptocurrencies are not regulated and do not benefit from the standard legal protections afforded by traded financial instruments. This leads to convoluted legal risks and inserts uncertainty, which can meaningfully influence both instability and risk management for these digital assets (Kang et al, 2021). There is also still no international consensus on how to best regulate cryptocurrencies (Yin et al, 2021).

Weakness 11: Diversity

Cryptocurrencies are qualitatively and technically diverse and incompatible. The various presently existing cryptocurrencies differ in several aspects, especially in terms of security, programmability, and governance characteristics (Valdeolmillos et al, 2019).

Weakness 12: Anonymity

To provide some form of privacy for users in the cryptocurrency ecosystem, cryptocurrencies like Bitcoin have designed their protocols to be pseudo-anonymous, where users use public key addresses to conduct their transactions rather than their actual real-world identities. Pseudonymity results in transactions being recorded as transfers of funds between one public key belonging to the payer to another public key belonging to the payee, thus preventing an observer from identifying the real-world identity of the payer and payee (Mnif, & Jarboui, 2021). However, complete anonymity opens the door to illicit activity that by definition cannot be investigated (Vukolić, 2015).

Weakness 13: The Technology Is Still Immature

According to Hughes et al (2019), cryptocurrencies are facing implementation obstacles beyond the lack of regulation and inactive obligations. Cryptocurrency and blockchain technology is emerging and is still immature in an ecosystem where other options are widely scalable and accepted over it. Kaur and Kaur (2020) also indicated that however long cryptocurrency technology has existed, not much has been done to expand it or enhance interoperability and legal use cases.

Weakness 5: Illiquidity and trading costs

In research to evaluate volatility connectedness in the cryptocurrency market, Yi et al (2018) found that the cryptocurrency market is generally less liquid. They indicated that the supply of many cryptocurrencies is controlled, with new units released according to a pre-set timetable, and it should thus come as no surprise that the high volatility of cryptocurrency prices is liquidity-driven. This constrains the ability of investors to exit from their cryptocurrency positions. In their findings also, part of the issue is that there is also no uniformity in the treatment of cryptocurrency trading since some exchanges incorporate the inherent features of cryptocurrencies, while others offer bilateral trading, with some replicating the core features of electronic trading platforms.

Weakness 6: Custody, clearing, and settlement problems

Besides further regulatory clarity, institutional custodial solutions for cryptocurrencies are both legally and technologically complicated. Pandya et al (2019) in their research to investigate cryptocurrency adoption efforts and security challenges in different countries found out part of the complexity is driven by the public and private key management. This research further indicated that the cryptographic keys need to be safeguarded and custodial solutions, therefore, must include multi-layered security features that appropriately manage and control how custodial systems can access, use and verify these keys. When these security measures are inadequate, disastrous results can ensue.

Weakness 7: Valuation difficulties

There is no consensus valuation approach, there are no commonly accepted metrics, and reported pricing information may differ substantively across venues (Schär,2020).

Weakness 8: Interoperability

The ability of blockchains and cryptocurrencies to see, access, and share information across different blockchains or blockchain networks is still limited (Fauzi et al, 2020). Interoperability enhances transparency and increases the communication rate of blockchains. Presently the technology has been divided to make multiple uses of it in different industrial domains and separate forms of cryptocurrencies. The technology needs to be made interoperable for the internet dedicated to Blockchain and crypto exchange (Pandya et al, 2019).

Weakness 14: Legal Obstacles

In addition to the lack of legislation, the other big obstacle that stands in the way of cryptocurrency holders like Bitcoin traders and users is the challenge to spend their holdings (Sharma et al, 2020).

Weakness 15: Usability

While cryptocurrency promises that it's accessible and decentralized, its complexity is restricting its user base to a narrow, homogeneous set of early adopters. According to Qureshi et al, (2020), Usability is one of the huge obstacles that hinder the cryptocurrency's path to mainstream adoption.

Weakness 16: Bad Imagery

The cryptocurrency industry association with shady business practices, high-profile hacks, environmental challenges, speculation, market manipulation, criminal associations, and a pronounced lack of regulatory clarity have created a perception and image problem (Bez et al, 2019).

Weakness 17: Data and modeling obstacles

There is no necessary data to model the future of cryptocurrencies. The detailed but narrow data set of actual transaction prices that cryptocurrency markets provide is inadequate for modeling purposes (Teker et al, 2020).

Weakness 18: expensive Mining process

Cryptocurrency mining is energy-intensive and makes the mining process to be expensive. The amount of electricity used to mine bitcoin according to Bouri et al (2019) has historically been high compared to any other usage in most countries.

Table 2: Cryptocurrency weaknesses derived from the literature source: (author).

SN	Cryptocurrency Weakness	Description	Weight out of 66	Percentage mentioned
1.	Highly Volatile	Cryptocurrency prices are highly volatile, responding strongly to global events and speculative concerns about the cryptocurrency market.	66	100%
2.	Conversion issues	Conversion remains a huge hurdle for Bitcoin vendors. As Bitcoin is not a fiat currency and is only limited to monetary value when converted to a cash equivalent, not many	61	92.42%

		vendors go for its conversions for other cryptocurrency types.		
3.	Scalability	Cryptocurrencies are less scalable	59	89.39%
4.	Lack of Legislation	Digital currencies are decentralized virtual entities. They are purely digital products, and authorities are currently not geared to handle this advanced technology. Therefore, the lack of legislation regulating these digital currencies and providing any sort of user protection has become a huge challenge.	52	78.79%
5.	Illiquidity and trading costs	The cryptocurrency market is generally less liquid	51	77.27%
6.	Custody, clearing, and settlement problems	Institutional custodial solutions for cryptocurrencies are both legally and technologically complicated.	49	74.24%
7.	Valuation difficulties	There is no consensus valuation approach, there are no commonly accepted metrics, and reported pricing information may differ substantively across venues.	45	68.18%
8.	Interoperability	The technology needs to be made interoperable for the internet dedicated to Blockchain and crypto exchange.	41	62.12%
9.	Cryptocurrencies are unpopular	The willingness of parties to accept the cryptocurrency as a standard of value in their mutual dealings is still an issue	32	48.48%
10.	Regulatory and Legal Dilemmas	cryptocurrencies are not regulated products and do not benefit from the standard legal protections afforded traded financial instruments.	27	40.91%
11.	Diversity	Cryptocurrencies are qualitatively diverse and not interchangeable (cryptocurrencies differ)	25	37.88%
12.	Anonymity	A problem for combating money laundering and countering terrorist financing or tax evasion	20	30.30%
13.	The Technology Is Still Immature	The technology is emerging and still immature in a system where other options are widely scalable and accepted over it.	20	30.30%
14.	Legal Obstacles	In addition to the lack of legislation, the other big obstacle that stands in the way of cryptocurrency holders like Bitcoin traders and users is the challenge to spend their holdings.	19	28.79%
15.	Usability	Buying and selling cryptocurrencies currently are difficult	15	22.73%
16.	Bad Imagery	Cryptocurrency still has a PR problem.	12	18.18%
17.	Data and	The detailed but narrow data set of actual	09	13.64%

	modeling obstacles	transaction prices that cryptocurrency markets provide is inadequate for modeling purposes.		
18.	Mining process	The mining process in cryptocurrencies takes up more electricity bills	03	4.55%

6.0 CONCLUSION

The results of this analysis as shown above indicated that there are several weaknesses in the present cryptocurrencies. To enhance visualization and interpretation, the 18 weaknesses are briefly described and presented in the matrix Table xx below. The frequency to show several sources that mentioned each weakness and the percentage concerning all reviewed papers before reaching theoretical saturation. Although research shows that Distributed Ledger Technology (DLT) and cryptocurrencies open up many opportunities, such as fast, efficient, traceable, and secure local and cross-border transactions, the above challenges must be addressed.

REFERENCES

1. B. Rawat, D., Chaudhary, V., & Doku, R. Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems. Journal of Cybersecurity and Privacy, 2020; 1(1): 4-18.
2. Baillon, A. (August). Follow the money: Bayesian Markets to aggregate expert opinions when the majority can be wrong. *In Workshop on Fintech and Machine Learning*, 2019; 5(8).
3. Bayram, O. Importance of Blockchain use in cross-border payments and evaluation of the progress in this area. *Doğuş Üniversitesi Dergisi*, 2020; *21*(1): 171-189.
4. Bez, M., Fornari, G., & Vardanega, T. (April). The scalability challenge of ethereum: An initial quantitative analysis. In *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, 2019; 167-176. IEEE.
5. Bouri, E., Lau, C. K. M., Lucey, B., & Roubaud, D. Trading volume and the predictability of return and volatility in the cryptocurrency market. *Finance Research Letters*, 2019; *29*: 340-346.
6. Bullmann, D., Klemm, J., & Pinna, A. In search for stability in crypto-assets: are stablecoins the solution?. *ECB Occasional Paper*, 2019; 230.
7. Brown, J. V., Crampton, P. E., Finn, G. M., & Morgan, J. E. From the sticky floor to the glass ceiling and everything in between: protocol for a systematic review of barriers and

facilitators to clinical academic careers and interventions to address these, with a focus on gender inequality. *Systematic reviews*, 2020; *9*(1): 1-7.

8. CoinMarketCap. (2 25). *CoinMarketCap*. Retrieved from Today's Cryptocurrency Prices by Market Cap: https://coinmarketcap.com/, 2021.
9. Dennis, R., & Disso, J. P. An analysis into the scalability of bitcoin and ethereum. In *Third International Congress on Information and Communication Technology*, 2019; 619-627. Springer, Singapore.
10. Ding, M., Soderberg, L., Jung, J. H., & Dahm, P. Low Methodological Quality of Systematic Reviews Published in the Urological Literature (2016-2018). *Urology*, 2020; *138*: 5-10.
11. FAUZI, M. A., PAIMAN, N., & OTHMAN, Z. Bitcoin and cryptocurrency: Challenges, opportunities and future works. *The Journal of Asian Finance, Economics, and Business*, 2020; *7*(8): 695-704.
12. Gorbunova, M., Masek, P., Komarov, M., & Ometov, A. (2021). Distributed ledger technology: State-of-the-art and current challenges. Computer Science and Information Systems.
13. Huang, Y., Wang, H., Wu, L., Tyson, G., Luo, X., Zhang, R., & Jiang, X. Characterizing eosio blockchain. *arXiv preprint arXiv:2002.05369*, 2020.
14. Kang, H. J., Lee, S. G., & Park, S. Y. Information Efficiency in the Cryptocurrency Market: The Efficient-Market Hypothesis. *Journal of Computer Information Systems*, 2021; 1-10.
15. Long, H. A., French, D. P., & Brooks, J. M. Optimising the value of the critical appraisal skills programme (CASP) tool for quality appraisal in qualitative evidence synthesis. *Research Methods in Medicine & Health Sciences*, 2020; *1*(1): 31-42.
16. McCarthy, B., Trace, A., O'Donovan, M., Brady-Nevin, C., Murphy, M., O'Shea, M., & O'Regan, P. Nursing and midwifery students' stress and coping during their undergraduate education programmes: An integrative review. *Nurse education today*, 2018; *61*: 197-209.
17. Min, H. Blockchain technology for enhancing supply chain resilience. *Business Horizons*, 2019; *62*(1): 35-45.
18. Mnif, E., & Jarboui, A. Resilience of Islamic cryptocurrency markets to Covid-19 shocks and the Federal Reserve policy. *Asian Journal of Accounting Research*, 2021.
19. Moin, A., Sekniqi, K., & Sirer, E. G. SoK: A classification framework for stablecoin designs. In Financial Cryptography, 2020.

20. Pandya, S., Mittapalli, M., Gulla, S. V. T., & Landau, O. Cryptocurrency: Adoption efforts and security challenges in different countries. *HOLISTICA–Journal of Business and Public Administration*, 2019; *10*(2): 167-186.
21. Qureshi, S., Aftab, M., Bouri, E., & Saeed, T. Dynamic interdependence of cryptocurrency markets: An analysis across time and frequency. *Physica A: Statistical Mechanics and its Applications*, 2020; *559*: 125077.
22. Schär, F. Decentralized Finance: On Blockchain-and Smart Contract-based Financial Markets. *Available at SSRN 3571335*, 2020.
23. Sharma, G. D., Jain, M., Mahendru, M., Bansal, S., & Kumar, G. Emergence of Bitcoin as an investment alternative: A systematic review and research agenda. *International Journal of Business and Information*, 2019; *14*(1): 47-84.
24. Sitienei, L. C. *An Assessment of the challenges affecting electricity transmission network expansion in Kenya; a case study of KETRACO* (Doctoral dissertation, Strathmore University), 2020.
25. Teker, D., Teker, S., & Ozyesil, M. Macroeconomic Determinants of Cryptocurrency Volatility: Time Series Analysis. *Journal of Business & Economic Policy*, 2020; *7*(1): 65-71.
26. The Central Bank of Kenya (CBK). (2 22). *Discussion Paper on Central Bank Digital Currency*. Retrieved from Central Bank of Kenya: https://www.centralbank.go.ke/uploads/discussion_papers/CentralBankDigitalCurrency.pdf, 2022.
27. TradingView. (5 15). *Crypto market cap charts*. Retrieved from CRYPTOCURRENCY MARKET: https://www.tradingview.com/markets/cryptocurrencies/prices-all/, 2021.
28. Whittemore, R., & Knafl, K. The integrative review: updated methodology. *Journal of advanced nursing*, 2005; *52*(5): 546-553.
29. Yin, Y., Lv, D., Huang, X., Liu, J., Xie, S., & Zhang, Y. (December). Research on Blockchain Security Protection. In *2021 7th International Conference on Computer and Communications (ICCC)*, 2021; 1545-1550. IEEE.

APPENDIX XX: Conference Participation Certificate

Kenya Methodist University

Certificate of Participation

This is to certify that

Alex Kibet

Presented a paper on

A Systematic Review of Cryptocurrency Weaknesses

at the 9th Annual International Scientific Research Conference held on 6th & 7th July, 2022

Deputy Vice Chancellor,
Academic & Students Affairs

Director, Research, Innovation and Extension

APPENDIX XXI: Paper Publication Certificates

International Journal of Computer Science and Information Security

ISSN 1947 5500

IJCSIS July 2022 Volume 20 No. 7

This Research Publication Certificate

is presented to distinguished author

Alex KIBET

for peer-reviewed published paper entitled

" Design of A Model for Creating a Stable Cryptocurrency using Fiat Currency for Global Electronic Commerce "

Professor Ying Yang *Professor Yong Li* *Dr. Jorge A. Ruiz-Vanoye*

IJCSIS Editorial Board
International Journal of Computer Science and Information Security,
IJCSIS ISSN 1947-5500, Pittsburgh, PA, USA
Email: ijcsiseditor@gmail.com
http://sites.google.com/site/ijcsis/
https://google.academia.edu/JournalofComputerScience

11 August 2022

ISSN No. : 2321-9653

iJRASET

International Journal for Research in Applied Science & Engineering Technology

IJRASET is indexed with Crossref for DOI-DOI : 10.22214

Website : www.ijraset.com, E-mail : ijraset@gmail.com

ISRA Journal Impact Factor: **7.429**

45.98 INDEX COPERNICUS

THOMSON REUTERS

TOGETHER WE REACH THE GOAL

SJIF 7.429

Certificate

Editor in Chief, **iJRASET**