A BLOCKCHAIN-BASED MODEL FOR CURBING INSTITUTIONAL ACADEMIC CERTIFICATE FRAUD

ESTHER KABIBI NZARO

A THESIS SUBMITTED TO THE INSTITUTE OF COMPUTING AND INFORMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY OF TECHNICAL UNIVERSITY OF MOMBASA

2023

DECLARATION

This thesis is my original work and has not been presented for academic award in any other university.

Signature: _____ Date: _____

ESTHER KABIBI NZARO

MSIT/0009/2020

This thesis report has been submitted with our approval as University Supervisors.

Signature: _____ Date: _____

DR. KENNEDY ONDIMU

Institute of Computing and Informatics

Technical University of Mombasa

Signature: _____ Date: _____

DR. FULLGENCE MWAKONDO

Institute of Computing and Informatics

Technical University of Mombasa

DEDICATION

I dedicate this thesis to my family and friends. A special feeling of gratitude to my loving husband Benard for the great support and encouragement throughout my research. To my children: David, Faith, and Michael for being cooperative. I also dedicate this work to my friend Elizabeth for being there for me. Thanks to all my friends who supported and prayed with me

ACKNOWLEDGMENT

I would like to express my deep gratitude to the almighty God and all those who supported me. In particular, I offer my sincere gratitude to my supervisors, Dr. Kennedy Ondimu and Dr. Fullgence Mwakondo who guided me throughout the research. I also want to thank the Institute of Computing and Informatics team, for the encouragement and support accorded to me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
SHA 256	Secure Hash Algorithm
DPBFT	Delegated Practical Fault Tolerance
IPFS	Interplenary file system
API	Application Programming Interface
BMCIAF	Blockchain-based Model for Curbing Institutional Academic Certificate Fraud

DEFINATION OF KEY TERMS

Hashing:	Hashing is an algorithm that calculates a fixed-size bit string value from a file
Gas:	Gas is a unit of measurement unique to the ethereum blockchain that measures the computational work required to run a transaction
Fraud:	An act of deceiving or misrepresenting
Consensus:	A general agreement about something
Transaction:	A transaction usually means a sequence of information exchange and related work
Blockchain:	A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered
Internal fraud:	Occurs when an employee makes a false representation, fails to disclose information, or abuses a position of trust either for personal gain or to cause losses to others.
Smart contracts:	Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met
Ethical values:	Provide the moral compass by which we live our lives and make decisions.
Multi-signature:	Refers to requiring multiple keys to authorize a transaction

ABSTRACT

There is need for a certificate authentication mechanism in Africa to solve internal academic certificate fraud activities. This is because some fake certificates in circulation appear to be genuine but were obtained illegally from credible learning institutions. This is caused by an assumption that certificates being issued at the university are authentic. While authentication of the final academic certificate was studied in previous research, many researchers focused on securing the final academic certificate and assumed that all certificates issued by institutions were genuine thus creating a loophole for institutional academic certificate fraud. The purpose of this research was to develop a blockchain-based model that curbs institutional academic certificate fraud. The research target population was public universities in Kenya. Sampling was done using simple random sampling to identify universities to participate in the study. Secondary data was used to validate the model while primary data was used to construct the data mapping structure. Primary data was collected from the registry department and examination using questionnaires while secondary data was collected using document review.

Smart contracts were written using the GOLANG and deployed to the hypledger fabric. APIs are used to interact with the model to insert or retrieve data. The model has controls (smart contracts) to ensure a student goes through the entire learning process before he is awarded an academic certificate.

To validate the model, experiments were carried using the secondary data. The results of the experiments shows that the model prevents internal fraud by making sure that only students registered in the blockchain and who completed the academic requirements can receive their academic certificates. Verification of the academic certificate is done by simply scanning a QR Code embedded on the academic certificate using a developed mobile app. The model only validates certificates whose certificate information was generated by the model. Ensuring that certificates originating from universities are authentic will retain or increase the reputation and credibility of the institution. On the other hand, employers and other interested parties will also give jobs to qualified people thus increasing the throughput and general job performance.