

**A BLOCKCHAIN IMPLEMENTATION MODEL FOR ELECTRONIC
VOTING SYSTEM**

**APEH, JONATHAN APEH
(15PCH01171)**

OCTOBER, 2022

**A BLOCKCHAIN IMPLEMENTATION MODEL FOR ELECTRONIC
VOTING SYSTEM**

BY

**APEH, JONATHAN APEH
(15PCH01171)**

**B.Sc (Hons.) Computer Science, Benue State University, Makurdi
M.Sc Advanced Software Engineering, Westminster University, London**

**A THESIS SUBMITTED TO THE SCHOOL OF POSTGRADUATE
STUDIES IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR
THE AWARD OF THE DEGREE OF DOCTOR OF PHILOSOPHY (Ph.D)
IN MANAGEMENT INFORMATION SYSTEM IN THE DEPARTMENT OF
COMPUTER AND INFORMATION SCIENCES, COLLEGE OF SCIENCE
AND TECHNOLOGY, COVENANT UNIVERSITY, OTA, OGUN STATE,
NIGERIA**

OCTOBER, 2022

ACCEPTANCE

This is to attest that this thesis is accepted in partial fulfillment of the requirements of the award of the degree of Doctor of Philosophy (Ph.D) in Management Information Science in the Department of Computer and Information **Sciences**, College of Science and Technology, Covenant University, Ota, Ogun State, Nigeria.

Miss. Adefunke F. Oyinloye
(Secretary, School of Post Graduate Studies)

Signature and Date

Prof. Akan B. Williams
(Dean, School of Post Graduate Studies)

Signature and Date

DECLARATION

I, **APEH, JONATHAN APEH (15PCH01171)**, declare that this research was carried out by me under the supervision of Professor Charles K. Ayo of the Department of Computer Science, Trinity University, Yaba, Nigeria, and Professor Ayodele A. Adebisi of the Department of Computer Science, Landmark University, Omu-Arun, Nigeria. I attest that the thesis has not been presented either wholly or partly for the award of any degree elsewhere. All sources of data and scholarly information used in this thesis are duly acknowledged.

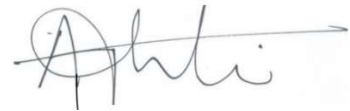
APEH, JONATHAN APEH

Signature and Date

CERTIFICATION

We certify that the thesis titled “**A BLOCKCHAIN IMPLEMENTATION MODEL FOR ELECTRONIC VOTING SYSTEM**” is an original research work carried out by **APEH, JONATHAN APEH (15PCH01171)**, in the Department of Computer and Information Sciences, Covenant University, Ota, Ogun State, Nigeria, under the supervision of Professor Charles K. Ayo and Professor Ayodele A. Adebisi. We have examined and found the work acceptable as part of the requirements for the award of Doctor of Philosophy (Ph.D) degree in Management Information System.

Prof. Charles K. Ayo
(Supervisor)



Signature and Date

Prof. Ayodele A. Adebisi
(Co-Supervisor)



Signature and Date

Prof. Olufunke O. Oladipupo
(Head of Department)

Signature and Date

Prof. Adesina S. Sodiya
(External Examiner)

Signature and Date

Prof. Akan B. Williams
(Dean, School of Postgraduate Studies)

Signature and Date

DEDICATION

I dedicate this thesis to my Heavenly Father – the source of wisdom and in whom is no variation or shadow of turning. I also dedicate it to my wife Mrs. Eunice Apeh and my daughters Jewel and GodsHeir; my dad Elder Matthew E. Apeh, my mum Mrs. Joy M. Apeh, and my brother Charles E. Apeh.

ACKNOWLEDGEMENTS

First, I acknowledge the inspiration of the Almighty God that gives understanding without which this thesis may never have been written. I wish to express my deep sense of gratitude and thanks to the Chancellor and Chairman of Board of Regents, Covenant University, Dr. David O. Oyedepo, for the academic and spiritual platform created. I sincerely thank the Pro-Chancellor, Bishop David Abioye, Vice-Chancellor, Professor Abiodun H. Adebayo, the Registrar, Mr Emmanuel Igban and the management team of Covenant University for running with the vision.

I acknowledge and thank Professor Akan B. Williams (Dean, School of Postgraduate Studies) for his leadership and huge support. I also heartily thank the staff of the postgraduate school for all the supports.

My thanks also go to Professor Olufunke O. Oladipupo (Head of Department, Computer and Information Sciences) for her quality leadership and management of all concerns.

I acknowledge and thank my supervisors, Professor Charles. K. Ayo and Professor Adebisi A. Ayodele for their mentoring and guidance whilst supervising this work. I thank God for the opportunity to have learnt from your wealth of experience and academic leadership up until now. I am certain your leadership, academic and research dexterity have rubbed off on me even as I move to accomplish higher things in the nearest future.

My special thanks to all members of Faculty of Computer and Information Sciences Department, Covenant University for their contribution, encouragement and support towards the realization of this thesis. Specifically, I appreciate profoundly the contributions and supports of associate Professor Aderonke A. Oni (former Postgraduate Coordinator, Department of Computer and Information Sciences) at every point all through. I am particularly thankful to Professor Ambrose Azeta for his invaluable support and guide and the host of others including Mr Opeyemi Olanipekun for all the supports in the validation process of this study.

Special thanks go to my family members both nuclear and extended who would not let me rest until I had completed the work satisfactorily. Foremost among whom are: My dad, elder Matthew E. Apeh, who encouraged me to pursue this dream and kept checking how I was progressing; my mum, Mrs. Joy. M. Apeh and my siblings for constant prayers, support and encouragement. God bless you. I deeply appreciate the unassuming love, prayers, understanding and all-round support of my wife, Mrs. Eunice. I. Apeh and our kids, Jewel and GodsHeir.

I would also like to thank all those people who contributed in some ways both directly and indirectly to the success of this research and writing of this thesis.

TABLE OF CONTENTS

COVER PAGE	i
TITLE PAGE	ii
ACCEPTANCE	iii
DECLARATION	iv
CERTIFICATION	v
DEDICATION	vi
ACKNOWLEDGEMENTS	vii
TABLE OF CONTENTS	ix
LIST OF FIGURES	xiii
LIST OF TABLES	xiv
LIST OF ABBREVIATIONS AND SYMBOLS	xv
ABSTRACT	xvii
CHAPTER ONE: INTRODUCTION	1
1.1. Background to the Study	1
1.2. Statement of the Problem	5
1.3. Aim and Objectives of the Study	6
1.4. Significance of the Study	6
1.5. Scope of the Study	7
CHAPTER TWO: LITERATURE REVIEW	8
2.1. Introduction	8
2.2. Electronic Voting(e-voting)	8
2.3. Electronic Voting Systems	9
2.3.1. Popular electronic voting system	14
2.3.2. Elections and Electronic Voting System in Nigeria’s Fourth Republic	18
2.3.3. E-voting System and Security Concerns	22
2.3.4. E-voting and Cryptography	23
2.4. Blockchain Technology	24
2.4.1 Hash Functions in Blockchain	24
2.4.2 Digital Signature in Blockchain	27

2.4.3. Blockchain Mechanism	28
2.4.4 Blockchain Architecture	30
2.4.5 Consensus Algorithms	31
2.4.6 Characteristics of Blockchain	34
2.4.7 Types of blockchain	37
2.4.8 Blockchain Application Areas	38
2.4.9 Blockchain Implementations	41
2.4.10 Challenges of Blockchain	49
2.5. Research Direction	59
2.6. Existing Latency and Scalability Implementations	61
2.6.1 Scalability	61
2.6.2 Latency	71
2.6.3 Electronic Voting System and Proposed Solutions to Cyber-threats	72
2.6.4 Blockchain-based Electronic Voting Systems	75
2.7 Summary	78
2.8 Deduction from Literature Review	79
CHAPTER THREE: METHODOLOGY	80
3.1. Introduction	80
3.2. Research Design	82
3.2.1. Data Collection	82
3.2.2. Questionnaire Validation	82
3.2.3. Design	84
3.2.4. Implementation Tool	88
3.2.5. Evaluation	92
3.3. Research Strategy	92
3.4. Research Instruments	92
3.5. Proposed Blockchain-based E-voting Model	93

3.5.1. System Architectural Design	95
3.5.2. Setting up the First Node on the Private Blockchain	98
3.5.3. Creating the Network	103
3.5.4. The Seed or Static Nodes	105
3.5.5. Creating the Decentralized Application	106
3.5.6. Deploying the Smart Contract	108
3.5.7. Deploying the Polling Units (PU) Module	110
3.5.8. Performance Impact of Proposed Model Design	116
3.5.8.1 Latency Evaluation	117
3.5.8.2. Scalability Evaluation	120
3.5.8.3. Usability Evaluation	122
3.6. Summary	126
CHAPTER FOUR: RESULTS AND DISCUSSION	127
4.1. Introduction	127
4.2. Scalability	127
4.3. Latency	129
4.4. Usability	134
4.5. Conclusion	136
CHAPTER FIVE: CONCLUSION AND RECOMMENDATION	137
5.1. Summary	137
5.2. Conclusion	138
5.3. Contributions to Knowledge	138
5.4. Recommendations	139
REFERENCES	140
APPENDICES	153
APPENDIX A	153

APPENDIX B	155
APPENDIX C	158
APPENDIX D	163

LIST OF FIGURES

FIGURES	LIST OF FIGURES	PAGES
1.1.	World Map of Electronic Voting (E-votingcc, 2018)	2
2.1:	How blockchain works	28
2.2:	The blockchain architecture	30
2.3:	Malleability Attack	55
2.4:	Sharding Architecture	66
3.1:	A model conceptualization of the methodology of the proposed blockchain model	82
3.2:	Keccak Sponge Function/construction	86
3.3:	Existing Blockchain based Electronic Voting System	95
3.4:	Proposed Blockchain-based E-Voting Model	96
3.5:	Blockchain-based E-Voting Model Design -Network view	97
3.6.	The blockchain nodes commandline environment	100
3.7:	Initialised node Geth Javascript environment	104
3.8:	PU Module directory structure	111
3.9:	eVoter web interface	113
3.10:	Voter's e-registration page	114
3.11:	Voter's dashboard	115
3.12:	Admin dashboard page	116
3.13:	Political position page	116
3.14:	MongoDB transactions cache	118
3.15:	Node1 with empty test.json file	120
3.16:	SUS representation on percentile ranks and grades	125
3.17:	Grades, adjectives, acceptability, and NPS categories associated with raw SUS scores	126
4.1.	proposed system's latency evaluation	132

LIST OF TABLES

TABLES	LIST OF TABLES	PAGES
	Table 2. 1: Hashing and blockchain structure	26
	Table 2. 2: Blockchain security features	36
	Table 2. 3: Blockchain classification by ownership	38
	Table 2. 4: Summary of top 4 blockchains: Bitcoin, Litecoin, Dogecoin, Ethereum	48
	Table 2. 5: Deductions from literature review	79
	Table 3. 1: Interview responses	83
	Table 3. 2: System Usability Scale	123
	Table 4. 1: The INEC SCR's setup time	127
	Table 4. 2: Evaluation of systems integrators' setup time	128
	Table 4. 3: Cost of deploying proposed model	129
	Table 4. 4: Latency (in ms) for blockchain cached state and HTTP request to an API server	130
	Table 4. 5: The Proposed model BEV System Usability Perception	135

LIST OF ABBREVIATIONS AND SYMBOLS

ACRONYMS	FULL MEANINGS
AES	Advanced Encryption Standard
ATM	Automated Teller Machine
BEL	Bharat Electronics Limited
BG	Byzantine Generals
BEV	Blockchain Electronic Voting
BTC	Bitcoin
BIP	Bitcoin Improvement Plan
CDH	Computational Diffie-Hellman Problem
DDCMs	Direct Data Capture Machine
DLT	Distributed Ledger Technology
DRE	Direct Recording Electronic
DiFi	Distributed Finance
DPoS	Delegated proof of stake
DDoS	Distributed Denial of Service
Dapp	Decentralized application
ECDSA	Elliptic Curve Digital Signature Algorithm
EOA	Externally Owned Account
EVM	Election Virtual Machine
ES&S	Electronic System and Software
INEC	Independent National Electoral Commission
PIN	Personal Identification Number
PoW	Proof of Work
PoS	Proof of Stake

PBFT	Practical Byzantine Fault Tolerance
JSON	JavaScript Object Notation
LTC	Litecoin
LCD	Liquid Crystal Display
LLL	Low-level Lisp-like Language
RSQ	Random Security Question
RSA	Rivest, Shamir, Adleman
RPC	Remote Protocol Call
OTP	One Time Password
PVC	Permanent Voters Card
PU	Polling Unit
SLA	Service Level Agreements
SPV	Simplified Payment Verification
SCR	Smart Card Reader
SIM	Subscriber Identification Module
SUS	System Usability Scale
TXID	Transaction Identity
TCP	Transmission Control Protocol
IoT	Internet of Things
TPS	Transactions per second
UPS	Uninterrupted Power Supply
VVPAT	Voter Verifiable Paper Audit Trail

ABSTRACT

The rate of Blockchain technology adoption is on the increase as seen in the cryptocurrency and Distributed Finance (DiFi) domain. The technology is also attracting lots of attention in many other application areas including the electronic voting(e-voting) system. The electronic voting system is an interesting use case for blockchain technology because critical problems within that space, specifically, the integrity of voting data, the secrecy of the ballot, and a single point of failure can be tackled with the technology. However, the scalability and latency of the blockchain network are two major challenges. This research, therefore, evolves a scalable, latency-improved blockchain implementation model for a Nation-Wide Electronic Voting System. The model is validated by a series of procedures: firstly, data collection, which involves observations, interviews, and the use of secondary data sources. The interview involved five Independent National Electoral Commission (INEC) personnel from the voters' education department and the Information and Communication Technology unit. Secondly, the model was designed using a combination of algorithm, software tools, and design decisions. The design decisions were built on the result of the analysis of four major blockchain networks (Bitcoin, Ethereum, Litecoin, and Dogecoin). Thirdly, the model implementation which is made of the steps taken to develop the proposed model. The implementation method includes setting up the node, creating a private blockchain network, creating a distributed application (DAPP) and the smart contract deployment. The Ethereum Virtual Machine, Solidity, and MongoDB were used to implement the model. The fourth procedure is the evaluation of the model performance from scalability, latency, and usability standpoints. The result from the latency evaluation showed a 99.36 percent improvement on the existing blockchain-based e-voting system; the scalability result shows the proposed model takes an average of 2.6 minutes to spin up a new node; the System Usability Scale (SUS) result shows a usability perception of 76 percent which is above average. The model therefore serves as a novel contribution to the application of blockchain technology to large scale e-voting like national election.

Keywords: Blockchain, Election Results Integrity. Electronic Voting System, INEC, Latency, Scalability.