

**DEVELOPMENT OF A DECENTRALISED MODEL FOR ELECTRONIC  
TICKETING USING BLOCKCHAIN TECHNOLOGY**

**OWIVRI, OGHENETEGA CHINEDU  
(21PCJ02285)**

**B.Eng. Electrical & Electronics Engineering, Kwame Nkrumah University of  
Science of Technology, Kumasi, Ghana**

**JULY, 2023**

**DEVELOPMENT OF A DECENTRALISED MODEL FOR ELECTRONIC  
TICKETING USING BLOCKCHAIN TECHNOLOGY**

**BY**

**OWIVRI, OGHENETEGA CHINEDU  
(21PCJ02285)**

**B.Eng. Electrical & Electronics Engineering, Kwame Nkrumah University of  
Science of Technology, Kumasi, Ghana**

**A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE  
STUDIES IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR  
THE AWARD OF MASTER OF ENGINEERING (M.Eng) DEGREE IN  
COMPUTER ENGINEERING IN THE DEPARTMENT OF ELECTRICAL  
AND INFORMATION ENGINEERING, COLLEGE OF ENGINEERING,  
COVENANT UNIVERISTY, OTA, OGUN STATE**

**JULY, 2023**

## **ACCEPTANCE**

This is to attest that this dissertation has been accepted in partial fulfillment of the requirements for the award of the degree of Master of Engineering in Computer Engineering in the Department of Electrical and Information Engineering, College of Engineering, Covenant University, Ota, Nigeria.

**Ms. Adefunke F. Oyinloye**  
**(Secretary, School of Postgraduate Studies)**

**Signature and Date**

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

**Signature and Date**

## **DECLARATION**

I, **OWIVRI, OGHENETEGA CHINEDU (21PCJ02285)**, declare that this dissertation is a representation of my work, and is written and implemented by me under the supervision of Dr. Kennedy O. Okokpujie of the Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria. I attest that this dissertation has not been submitted wholly or partially to any other university or institution of higher learning for the award of a master's degree. All information cited from published and unpublished literature has been duly referenced.

**OWIVRI, OGHENETEGA CHINEDU**

**Signature and Date**

## **CERTIFICATION**

We certify that this dissertation titled “**DEVELOPMENT OF A DECENTRALISED MODEL FOR ELECTRONIC TICKETING USING BLOCKCHAIN TECHNOLOGY**” is an original research work carried out by **OWIVRI, OGHENETEGA CHINEDU (21PCJ02285)**, in the Department of Electrical and Information Engineering, College of Engineering, Covenant University, Ota, Ogun State, Nigeria under the supervision of Dr. Kennedy Okokpujie. We have examined and found this work acceptable as part of the requirements for the award of Master of Computer Engineering.

**Dr. Kennedy O. Okokpujie**  
**(Supervisor)**

**Signature and Date**

**Dr. Isaac A. Samuel**  
**(Head of Department)**

**Signature and Date**

**Prof. Jonathan G. Kolo**  
**(External Examiner)**

**Signature and Date**

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

**Signature and Date**

## **DEDICATION**

All Glory to God Alone and my loving Mother Mrs. Josephine Ifeoma Owivri for her support, prayers, and for not giving up on me.

## ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude and appreciation to all those who have played a significant role in the completion of my thesis. Without their support, guidance, and encouragement, this accomplishment would not have been possible.

First and foremost, I am profoundly grateful to God for His grace, blessings, and unwavering guidance throughout this entire journey. His divine intervention has been instrumental in every step, and I am forever grateful.

I extend my deepest appreciation to my supervisor, Dr. Kennedy Okokpujie, for his continuous support, patience, and invaluable guidance. His expertise, constructive feedback, and motivation pushed me to strive for excellence and ensured that I met all the departmental deadlines. His unwavering belief in my abilities has been a driving force behind the successful completion of this thesis. I would like to extend my warmest appreciation to my internal assessor Dr. Oluwadamilola Oshin for her constructive criticisms, insights and contributions that have enhanced the quality of this research work.

I am grateful to Dr. Isaac Samuel, my Head of Department, for his words of encouragement and support, and I am grateful for his mentorship.

My heartfelt thanks go to my mother, Mrs. Josephine Ifeoma Owivri, for her prayers, unwavering support, and belief in my abilities. Her constant encouragement and love provided me with the strength and motivation to overcome obstacles along the way. I would also like to acknowledge my Aunt Adamma Duru for her encouraging words and unwavering support. Her belief in my potential and her constant motivation were instrumental in keeping me focused and determined.

Furthermore, I would like to express my gratitude to Sir Tarry for his valuable contributions to the development of this research work. His insights and expertise greatly enhanced the quality and depth of my research, and I am thankful for his contributions.

Finally, I extend my appreciation to all my friends and family members who have supported me throughout this journey. Your words of encouragement, understanding, and patience have been invaluable.

To all those mentioned and the countless others who have contributed in various ways, I am forever grateful for your support and guidance. Your presence in my life has been a tremendous blessing, and I am deeply indebted to each one of you. Thank you for believing in me and for being an integral part of my academic success.

## TABLE OF CONTENTS

CONTENT	PAGES
<b>COVER PAGE</b>	I
<b>TITLE PAGE</b>	II
<b>ACCEPTANCE</b>	III
<b>DECLARATION</b>	IV
<b>CERTIFICATION</b>	V
<b>DEDICATION</b>	VI
<b>ACKNOWLEDGEMENTS</b>	VII
<b>TABLE OF CONTENTS</b>	VIII
<b>LIST OF FIGURES</b>	X
<b>LIST OF TABLES</b>	XII
<b>ABBREVIATIONS</b>	XIII
<b>ABSTRACT</b>	XV
<b>CHAPTER ONE: INTRODUCTION</b>	1
1.1 Background to the Study	1
1.2 Statement of the problem	5
1.3 Research Questions	6
1.4 Aim and Objectives of the Research Work	6
1.5 Justification for the research	8
1.6 Scope of study	8
1.7 Research Limitations	8
<b>CHAPTER TWO: LITERATURE REVIEW</b>	9
2.1 Preamble	9
2.2 Origin of Blockchain	9
2.3 Asymmetric Cryptography and Digital Signature (ECDSA)	11
2.3.1 Digital signature algorithm	12
2.4 Hash Function	13
2.5 Secure Hash Algorithm (Keccak – 256)	14
2.6 Consensus Mechanism	15
2.6.1 Proof of work (PoW)	16
2.6.2 Proof of Stake (PoS)	17
2.6.2.1 Follow-the Satoshi (FTS) Algorithm	18
2.7 Ethereum Network	19
2.8 Electronic Ticketing	22
2.9 Ethereum Virtual Machine (EVM)	22
2.10 Smart Contracts (SC)	23
2.11 ERC Token Standard	25
2.12 IPFS (InterPlanetary File System)	26
2.13 QR code (Quick Response code)	27
2.14 Other Related Technologies	28
2.14.1 Metamask	28
2.14.2 Web 3.0	28
2.14.3 Decentralized Application (dApp)	28
2.14.4 React.JS	29



2.14.5 Thirdweb SDK	29
2.14.6 Sepolia Testnet	29
2.14.7 OpenZeppelin	30
2.15 Review of Related Works	30
2.16 Research gaps in related works	47
2.17 Performance Evaluation Metrics	48
<b>CHAPTER THREE: METHODOLOGY</b>	<b>49</b>
3.1 Preamble	49
3.2 System Architecture and Framework	51
3.3 Participants of the Proposed Ticketing Model	53
3.4 Solution to Traceability and Security	54
3.5 Evidence information for verification	55
3.6 Solution to privacy and transparency	58
3.7 Algorithm of the Ticketing Model	62
3.8 Smart Contract Deployment	63
3.9 Ticketing Smart Contract	64
<b>CHAPTER FOUR: RESULTS AND DISCUSSION</b>	<b>67</b>
4.1 Preamble	67
4.2 Implementation Details	67
4.3 Implementation Results of the Smart Contract Deployment	68
4.3.1 Data structures for ticket tracking	68
4.3.2 Data functions for ticketing smart contract	69
4.3.3 Compiling and deploying the smart contract to the EVM	74
4.4 Integrating the smart contract into a decentralized web application	76
4.4.1 Front-End UI of the dApp	76
4.4.2 Ticket Evidence Page	77
4.4.3 User Profile Page	77
4.5 Point of Admittance and Administrative client	78
4.6 Evaluation and Analysis	81
4.6.1 Security Analysis.	81
4.6.1.1 Integrity and Reliability	81
4.6.1.2 Trust	82
4.6.1.3 Security and Access Control	82
4.6.1.4 Privacy	82
4.6.2 Performance Evaluation	82
4.6.3 Benchmark Results with existing Works	84
<b>CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS</b>	<b>87</b>
5.1 Preamble	87
5.2 Summary	87
5.3 Research Contributions	87
5.4 Future Recommendations	88
<b>REFERENCES</b>	<b>89</b>
<b>APPENDIX A</b>	<b>93</b>
<b>APPENDIX B</b>	<b>100</b>

## LIST OF FIGURES

<b>FIGURES</b>	<b>TITLE OF FIGURES</b>	<b>PAGES</b>
1.1	Centralized Ticketing Architecture	3
2.1	PoW and PoS Comparison	19
2.2	Overview of the Ethereum Network	20
2.3	Overview of Smart Contracts	24
2.4	How Files are Stored on the IPFS	26
3.1	Research Activities Workflow	50
3.2	Overall Architecture of the Proposed Ticketing Framework	51
3.3	Transactions Hashed in a Merkle tree	55
3.4	Evidence for verification of ticket authenticity	57
3.5	Solution to Privacy and Transparency	59
3.6	Consumer ID Generation	60
3.7	Ticket Verify System	61
3.8	Check if The Regenerated Hash is Included in The Storage	62
3.9	Sequence Diagram of the Proposed Ticketing model	66
4.1	A screenshot of the login page of the dApp for electronic ticketing	67
4.2	Remix IDE	68
4.3	Code Snippet of the Mint Ticket Function	70
4.4	Snapshot of a successful ticket request transaction	71
4.5	Log of Tickets Marked as Used by the Administrative Client	72
4.6	Compilation results from Remix IDE	74
4.7	Thirdweb CLI for Uploading Smart Contract ABI to the Blockchain	75

4.8	Thirdweb SDK Dashboard for deploying Smart Contract	75
4.9	Front-End User Interface of the dApp	76
4.10	Ticket Evidence Page	77
4.11	User Profile Page on the dApp	78
4.12	Administrative Client for Point of Admittance	79
4.13	Transaction Log of all Tickets Marked as Used on the Administrative client	80
4.14	Administrative Dashboard for Tracking All Transactions on the SC	80
4.15	Arithmetic Mean and Median of the Ticket Purchase Completion Time	83
4.16	Arithmetic Mean and Median of the Ticket Verification Completion Time	84

## LIST OF TABLES

<b>TABLES</b>	<b>TITLE OF TABLES</b>	<b>PAGES</b>
1.1	Objectives and methodology mappings for the study	7
2.1	Literature Review Table	33
3.1	Standard fractions of Ether and their Wei Values	64
4.1	Classifications of SC Functions	73
4.2	Comparison of the proposed Model with Existing Works	86

## ABBREVIATIONS

<b>ABI</b>	Application Binary Interface
<b>CA</b>	Certificate Authority
<b>DAO</b>	Decentralized Autonomous Organizations
<b>DAPP</b>	Decentralized Applications
<b>DHT</b>	Distributed Hash Tables
<b>DOM</b>	Document Object Model
<b>DPoS</b>	Delegated Proof of Stake
<b>DSA</b>	Digital Signature Algorithm
<b>ECC</b>	Elliptic Curve Cryptography
<b>ECDSA</b>	Elliptic Curve Digital Signature Algorithm
<b>ERC</b>	Ethereum Request for Comments
<b>ETH</b>	Ether
<b>EVM</b>	Ethereum Virtual Machine
<b>FTS</b>	Follow-The-Satoshi
<b>ICT</b>	Information and Communication Technology
<b>IDE</b>	Integrated Development Environment
<b>IPFS</b>	Interplanetary File System
<b>JS</b>	JavaScript
<b>LPoS</b>	Leased Proof of Stake
<b>MITM</b>	Man in The Middle
<b>MSP</b>	Member Service Provider
<b>NFT</b>	Non-Fungible Token
<b>PoS</b>	Proof of Stake
<b>PoW</b>	Proof of Work
<b>QR</b>	Quick Response
<b>RSA</b>	Rivest Shamir Adleman
<b>SC</b>	Smart Contract
<b>SDK</b>	Software Development Kit
<b>SHA</b>	Secure Hash Algorithm

<b>TPS</b>	Transactions per Second
<b>TPM</b>	Transactions per Minute
<b>TX</b>	Transaction
<b>UI</b>	User Interface
<b>UTXO</b>	Unspent Transaction Output

## ABSTRACT

Single-user electronic ticketing systems are widely utilized in several industries, such as transportation, cafeterias, cinemas, and other activities but they face challenges such as fraud, counterfeiting, and security risks. This work addresses these issues by utilizing blockchain technology, which employs cryptography, decentralized ledgers, consensus mechanisms, and smart contracts. Existing electronic ticketing solutions often function in a centralized manner or focus solely on event-based ticketing, with limited progress in the context of single-user electronic ticketing systems. The proposed model leverages blockchain technology to ensure ticketing information transparency. It incorporates asymmetric encryption techniques to protect user privacy and utilizes digital signature technology to verify ticket authenticity. The model also introduces an innovative ticket verification mechanism using ERC721 standards. To achieve decentralization, the Ethereum Virtual Machine's request for comments (ERC-721) Protocols, digital signatures, and the Interplanetary File System (IPFS) are employed as decentralized storage for ticket metadata. This research not only addresses centralization concerns but also enhances security, traceability, transparency, and trust through the application of blockchain technology and cryptographic methods. The decentralized electronic ticketing model is implemented as a consumer application, and a comprehensive empirical analysis evaluates its performance, particularly in terms of transaction completion time. The outcomes illustrate the efficiency of the suggested model. in mitigating fraud, counterfeiting, and security risks in single-user electronic ticketing systems. The decentralized approach ensures improved reliability, security, and transparency. Based on the empirical analysis, the model exhibits efficient ticket transaction completion time of 19.64 seconds, and a mean ticket verification time of 3.17 seconds, providing a practical solution for real-world implementation. In conclusion, this research presents a robust and fully decentralized electronic ticketing model that leverages blockchain technology, ERC721 standards, digital signatures, and IPFS. The findings highlight the potential of the proposed model to revolutionize single-user electronic ticketing systems, fostering security, reliability, and trust in ticketing transactions.

***Keywords: Blockchain, Cryptography, ERC721, EVM, Smart Contract, Ticketing***