

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



Sudan University of Science And Technology



College of Graduate Studies

Master of Information Technology Program

**A proposed Electronic Voting System Based on Block Chain Technology
By Application on the National Electoral Commission of Sudan**

مقترح نظام إلكتروني مبني على تقنية البلوك تشين بالتطبيق على المفوضية القومية
للانتخابات بالسودان



*A Thesis Submitted In Partial Fulfillment of
The Requirements For The Degree of
Master of Information Technology*

By :
Mohamed El-fatih Hayder Salih Hussain

Supervised :
Dr. Faisal Mohamed Abdallah Ali

December 2020

Dedications

This research is dedicated to:

The sake of Allah, my Creator and my Master, My great teacher and messenger, Mohammed (May Allah bless And grant him) who taught us the purpose of life, Sudan University of Science and Technology, my second magnificent home, My great parents, who devoted themselves helped to get this point My beloved brothers and sisters , My beloved family Who always can be with me. And my bosom friends who encourage and support me, All the people in my life who touch my heart I dedicate this research.

Acknowledgment

In the name of Allah the Merciful Praise be to Allah. And blessings and peace be upon Muhammad Abdullah and his Messenger. First and foremost, I must confess unlimited thanks to Allah , the greatest and most thankful, for his help and blessings. I am absolutely sure this business would never have been possible without his guidance. I owe a deep debt of gratitude to our university for giving us an opportunity to complete this work. I am grateful to the colleges that worked hard with me from the beginning until the completion of this research especially my supervisor Dr. Faisal Mohamed Abdullah, who was always generous throughout the research period, and I greatly appreciate the efforts he made. I would like to take this opportunity to express my warm thanks to my sheikh and mentor Sheikh Dr. Muhammad Shaykh Hassan El- Fatih Qaribullah , the general guide of the nearby Samanyia Al-Tayyibia method and to all my friends and who were supportive throughout the path of conducting this research. I would also like to express my sincere thanks to my family for their generous support that they have provided me throughout my entire life especially through the process of pursuing a master's degree. Because of their unconditional love and prayers, I have a chance to complete this research. Thanks is not enough to all my colleagues and all the people who gave me a lot, long hours of their time helped me in my research, especially to all members of the postgraduate studies at Sudan University of Science and Technology.

Abstract

Elections are the essential part of every democratic society and organization. Hence it is very important to hold up as many elections as possible. Manual voting has been replaced by electronic machines called electronic voting machines (EVM). Even after the replacement, security problems persisted in electronic systems, such as hackers infiltrating the system, tampering with vote count results, and a lack of credibility and transparency, raising voter concerns. And other matters such as losing names on the voters' roll and impersonating the voter and voting instead. To solve all these problems and others, A proposed a decentralized system that integrates with the electronic voting system to be free from errors. One of those decentralized systems is block chain technology. The proposed system was developed on the Ethereum platform using the Solidity language. The block chain based electronic voting system needs to ensure that the election result is largely canceled. Voters were encrypted and stored in the database by choosing the AES algorithm to encrypt and decrypt the vote, verify voters using a fingerprint in addition to their national number, thus securing all voting steps, ensuring confidentiality, authentication and privacy in the electoral process. Finally, a security analysis was performed to show how the proposed model can resist attacks, address various vulnerabilities, and thus have satisfactory results in providing the necessary security in all transactions between the voter and the server.

المستخلص

الانتخابات هي الجزء الأساسي لكل مجتمع ومنظمة ديمقراطية. ومن ثم فمن المهم للغاية إجراء أكبر عدد ممكن من الانتخابات ، تم استبدال التصويت اليدوي بآلات إلكترونية تسمى آلات التصويت الإلكترونية (EVM) حتى بعد الاستبدال ، استمرت المشكلات الأمنية في الأنظمة الإلكترونية مثل اختراق الهاكرز للنظام ، والتلاعب بنتائج فرز الأصوات ، وانعدام المصادقية والشفافية ، مما أثار المخاوف لدى الناخبين ، وقضايا أخرى مثل فقدان الأسماء في قائمة الناخبين ، وانتحال شخصية الناخب، والتصويت بدلا عنه . لحل كل هذه المشكلات وغيرها أفرح نظامًا لا مركزيًا يتكامل مع نظام التصويت الإلكتروني لجعله خاليًا من الأخطاء. واحدة من تلك الأنظمة اللامركزية هي تقنية البلوك تشين تم تطوير النظام المقترح على منصة الإثيريوم باستخدام لغة Solidity . يحتاج نظام التصويت الإلكتروني القائم على تقنية البلوك تشين إلى ضمان القضاء على إمكانية التلاعب بنتيجة الانتخابات إلى حد كبير. تم تشفير الناخبين وتخزينهم في قاعدة البيانات عن طريق اختيار خوارزمية AES لتشفير وفك تشفير التصويت ، والتحقق من الناخبين باستخدام بصمة الإصبع بالإضافة إلى رقمهم الوطني ، وبالتالي تأمين جميع خطوات التصويت ، وضمان السرية والمصادقة والخصوصية في العملية الانتخابية. أخيرًا ، تم إجراء تحليل أمني لإظهار كيف يمكن للنموذج المقترح مقاومة الهجمات ومعالجة نقاط الضعف المختلفة وبعد ذلك تحصلت على نتائج مرضية في توفير الأمان اللازم في جميع المعاملات بين الناخب والخدم.

List of Contents

Contents	Page No
Dedications	II
Acknowledgement	III
Abstract	IV
Abstract (Arabic)	V
List of Contents	VI
List of Tables	IX
List of Figures	X
List of Abbreviation	XIII
1. Chapter One Introduction	
1.1 Background	1
1.2 Research Motivation	2
1.3 Problem statement	2
1.4 Objective	2
1.5 Research methodology	3
1.6 Research Important	3
1.7 Thesis Layout	3
2. Chapter Two Literature Review	
2.1 Introduction	5
2.1.1 Internet	5
2.1.2 E- Government	6
2.1.3 E-Services	6
2.2 The importance of voting	6
2.2.1 Traditional Voting System	7
2.2.2 Some of the problems facing traditional voting	9
2.2.3 Electronic Voting System	9

Contents	Page No
2.2.4 Block chain in E-Voting System	10
2.3 Block chain Explained	10
2.3.1 Block chain History	11
2.3.2 Type of Block chain	11
2.3.3 Block chain components	12
2.3.4 Block Chain Consists	16
2.3.5 How the Block chain Works	17
2.3.6 Benefits of the Block chain technology	17
2.3.7 Block chain Application and use cases	17
2.4 Examples of countries using block chain in E-voting system	19
2.4.1 Estonian E-Voting System	19
2.4.2 Domestic Online Voting System K-Voting	21
2.4.3 Republican Presidential Nomination in Utah , US	21
2.5 Existing Block chain Platforms	22
2.6 Smart Contract Technology	24
2.7 Block chain As a services on E-voting system	29
2.8 Block chain As a services on E-voting system Using Ethereum	30
2.9 E-voting System Related Works	32
2.10 Related Work Applications	33
3. Chapter Three Research Methodology	
3.1 Introduction	36
3.2 Block Chain E-voting System Requirements	36
3.3 Representation of the E-voting System	37
3.4 Mechanisms of E-voting system	38
3.5 Block Chain E-Voting System Architecture	38
3.6 Data Flow diagram	45
3.6.1 Registration phase	45
3.6.1 Registration phase	46
3.7 Unified Modeling Language (UML) Analysis	47

Contents	Page No
3.7.1 Use case diagrams	47
3.7.2 Sequence diagrams	48
3.8 Designing stage	51
3.8.1 Create tables inside the new database	51
3.8.2 Design Category Diagram	54
4. Chapter Four Implementation	
4.1 Introduction	58
4.2 Overview of The Secure Electronic Voting Using Block chain	58
4.2.1 Registration Phase	58
4.2.2 Voting Phase	63
4.2.3 Admins page	73
4.2.4 Result phase	81
4.3 Security analysis and Results	85
4.3.1 Potential attacks	85
4.4.2 Results	86
5. Chapter Five Conclusion And Recommendation	
5.1 Conclusion	88
5.2 Recommendation	89
References	90

List of Tables

Table	Page No
Table 2.1 E-Voting Systems Deployed All Over the World	34
Table 3.1 Example of an transaction in our system	41
Table 3.2 Candidate table	51
Table 3.3 parties table	52
Table 3.4 Result table	52
Table 3.5 State table	52
Table 3.6 Users table	53
Table 3.7 voter table	53

List of Figures

Figures	Page No
Fig. 2.1 Block chain component components	12
Fig. 2.2 A schematic of double envelope encryption	13
Fig. 2.3 Basic Function of the SHA-256	13
Fig.2.4 One block (nodes)on the block chain	14
Fig.2. 5 Creation of new Block containing a Hash Value	14
Fig. 2.6 Header and Body on the block	15
Fig. 2.7 Block chain	16
Fig.2. 8 Block chain Works	16
Fig.2.9 Block chain cryptocurrencies	18
Fig. 2.10 Estonian E-voting system	20
Fig. 2.11 Comparison of features in popular block chain	24
Fig. 2.12 Working of Smart contracts	26
Fig. 2.13 Block chain As a services on E-voting system	30
Fig. 2.14 Representation of Truffle Framework	31
Fig. 2.15 Overview of Web3.js	32
Fig.2. 16 Illustration of client side application using SC	32
Fig. 3.1 A Simple Requirement of the Block chain Structure	36
Fig. 3.2 A Simple Representation of the Block chain Structure	37

Figures	Page No
Fig. 3.3 Registration phase	39
fig. 3.4 Pallote phase	42
fig. 3.5 DFD register phase	45
fig. 3.6 DFD Polling phase	46
Fig. 3.7 use case of voters login	47
Fig. 3.8. use case of admins process	47
Fig. 3.9. sequence of login voter	48
Fig. 3.10. sequence voting process	49
Fig. 3.11. sequence of election result process	50
Fig. 3.12 manage from candidate page	54
Fig. 3.13 manage from parties page	54
Fig. 3.14 manage from state page	54
Fig. 3.15 manage from voter page	55
Fig. 3.16 and Fig .3.17 manage from Admin	55
Fig. 3.18 Relational schema tables	56
Fig. 4.1 Registration login	59
Fig. 4.2 Insert ID_Num and scan Finger print	60
Fig. 4.3 The system verify information	60
Fig. 4.4 information of voter	61
Fig. 4.5 system give voter Reg_num	61
Fig. 4.6 to Fig 4.8 recovery Reg_num	62
Fig. 4.9 Error message from system to voter	63

Figures	Page No
Fig. 4.10 to Fig 4.11 voting login page	64
Fig. 4.12 to Fig 4.13 vote page	65
Fig. 4.14 to Fig 4.22 Block chain transaction hash	66
Fig. 4.23 successful vote page	71
Fig. 4.24 validation page	71
Fig. 4.25 AES algorithms Result in DB	72
Fig. 4.26 End of vote phase	72
Fig. 4.27 Admin login	73
Fig. 4.28 to Fig 4.45 Admins page	74
Fig. 4.46 to Fig 4.54 Result page	81

List of Abbreviation

AS : Authentication Server

CIO : Chief Information Officer

CRUD : Create, Read, Update and Delete

D-Apps : Decentralized application

DLT : Distributed ledger technology

EMB: Election Management Body

ESD : Electronic Service delivery

EVS : Electronic Voting System

ICT: Information Communication Technology

NEC : National Elections Commission

PBFT: Practical Byzantine Fault Tolerance

TDS : Token Distribution Server

TTP: Trusted Third Party

UML: Unified Modelling Language