بسم الله الرحمن الرحيم

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 للإنتخابات 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 المصداقية 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 أقترح 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 الإثريوم 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 والخادم.

List of Contents

Contents **Page No**

Contents **Page No**

List of Tables

List of Figures

Figures **Page No**

Figures **Page No**

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