FINAL YEAR PROJECT REPORT

BLOCKCHAIN-POWERED VOTING WITH FINGERPRINT AUTHENTICATION

In fulfillment of the requirement
For degree of
BS (COMPUTER SCIENCES)

By

WALEED MUHAMMAD	73235 (BSCS)
FURQAN ZAKA UD DIN	73040 (BSCS)
ABDULLAH MASHOOD JAFRI	82094 (BSCS)

SUPERVISED

BY
MS.AZEEMA SADIA

BAHRIA UNIVERSITY (KARACHI CAMPUS)

FALL-2024

DECLARATION

We hereby declare that this project report is based on our original work except for citations and quotations which have been duly acknowledged. We also declare that it has not been previously and concurrently submitted for any other degree or award at Bahria University or other institutions.

Signature : _____

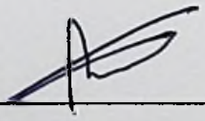
Name : Waleed Muhammad

Reg No. : 73235

Signature : Furqan _____

Name : Furqan Zaka Ud Din

Reg No. : 73040



Signature : _____

Name : Abdullah Mashood Jafri

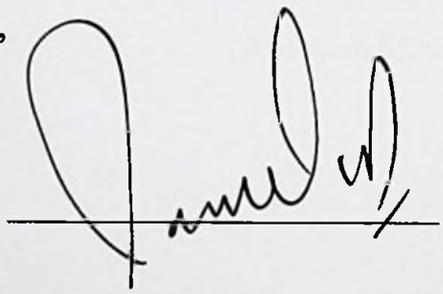
Reg No. : 82094

Date : 8th-December-2024

APPROVAL FOR SUBMISSION

We certify that this project report entitled **"BLOCKCHAIN-POWERED VOTING WITH FINGERPRINT AUTHENTICATION"** was prepared by **Waleed Muhammad, Furqan Zaka Ud Din** and **Abdullah Mashood Jafri** has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Science in **Computer Science** at Bahria University, Karachi.

Approved by,

Signature : 

Supervisor : Miss Azeema Sadia

Date : 3th December-2024

Specially dedicated to

My beloved parents & teachers

(Waleed Muhammad)

My beloved mother & father

(Furqan Zaka Ud Din)

My beloved grandparents & parents

(Abdullah Mashood Jafri)

ACKNOWLEDGEMENTS

We would like to thank everyone who had contributed to the successful completion of this project. We would like to express my gratitude to my project supervisor, Miss Azeema Sadia for her invaluable advice, guidance and her enormous patience throughout the development of the research.

In addition, we would also like to express our gratitude to our loving parents and friends who have helped and given us encouragement.

BLOCKCHAIN-POWERED VOTING WITH FINGERPRINT AUTHENTICATION

ABSTRACT

This project presents a comprehensive approach to creating a secure, transparent, and user–friendly voting platform that leverages the strengths of modern blockchain technology and sophisticated authentication mechanisms. By employing Ethereum smart contracts, all voting data is recorded in an immutable ledger that preserves the integrity of election information and mitigates the risk of tampering. The platform not only allows administrators to establish campaigns and register candidates with confidence but also ensures that voters can cast their ballots without fear of manipulation.

To enhance the overall security and user experience, the system integrates both conventional password–based authentication and advanced WebAuthn credentials. This dual–method approach recognizes that while some users prefer familiar login credentials, others value the added protection that biometric verification and hardware–bound credentials can provide. A Python–based application programming interface interacts seamlessly with a database, preserving sensitive user information and fingerprint data with a high level of confidentiality. Meanwhile, a Node.js server orchestrates communication among the blockchain network, the backend services, and the browser–based frontend interface. Through these carefully designed interactions, participants enjoy a cohesive, secure, and accessible voting environment.

Rigorous testing procedures and evaluations confirm that this decentralized solution not only strengthens trust through verifiable on–chain transactions but also streamlines the voting process. By reducing reliance on centralized authorities and introducing robust safeguards against fraud, the platform empowers communities to hold elections that are both technologically sophisticated and socially accountable. The result is a blueprint for future electoral systems that prioritize transparency, security, and inclusivity at every stage.

TABLE OF CONTENTS

DECLARATION	ii
APPROVAL FOR SUBMISSION	iii
ACKNOWLEDGEMENTS	v
ABSTRACT	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	xi
LIST OF FIGURES	xii
LIST OF SYMBOLS / ABBREVIATIONS	xiii
LIST OF APPENDICES	xiv

CHAPTER

1	**INTRODUCTION**		1
	1.1	**Background**	1
	1.2	**Problem Statement**	2
	1.3	**Aims and Objectives**	4
		1.3.1 Managed Election through Smart Contracts	4
		1.3.2 Powerful Authentication Measures	4
		1.3.3 Securing User Data and Data Privacy	5
		1.3.4 Make an Easy-to-Use Interface Design	5
		1.3.5 Voting and Election participation easily with Verification	5
		1.3.6 Check Voter System Performance, Security, and Reliability	5
	1.4	**Scope of Project**	6
		1.4.1 Blockchain-Based Voting Platform	6
		1.4.2 Secure Voter Authentication	6
		1.4.3 System Architecture and Components	7
		1.4.4 Testing and Validation	7
		1.4.5 Demonstration and Limitations	7
		1.4.6 Future Considerations	8

2	**LITERATURE REVIEW**		**9**
	2.1	**Blockchain for Secure Voting**	**9**
	2.2	**WebAuthn and Password Authentication**	**10**
	2.3	**Assessment of Blockchain-based Voting Governance Smart Contracts Security**	**11**
		2.3.1 Access Control Evaluation	11
		2.3.2 Data Integrity and Immutability	11
	2.4	**Existing Systems and Research Gaps**	**12**
3	**REQUIREMENT SPECIFICATIONS**		**14**
	3.1	**Existing System**	**14**
		3.1.1 Verifying the Identity of Voter	14
		3.1.2 Auditability and Transparency	14
		3.1.3 Global cybercrimes have security implications	15
	3.2	**Proposed System**	**15**
		3.2.1 Blockchain Voting	15
		3.2.2 Dual Way Authentication	16
		3.2.3 Improved Transparency	16
		3.2.4 Improved Security	16
		3.2.5 Improved UI	16
	3.3	**Requirement Specifications**	**17**
		3.3.1 Functional Requirements	17
		3.3.2 Non-Functional Requirements	18
		3.3.3 Use Cases	21
4	**DESIGN AND METHODOLOGY**		**24**
	4.1	**Methodology (Frame of Work/Architecture)**	**24**
		4.1.1 Layer 1- Blockchain Layer	24
		4.1.2 Layer 2- Backend Layer	24
		4.1.3 Layer 3- Frontend Layer	24
	4.2	**Process Model**	**25**
		4.2.1 Requirements Gathering	25
		4.2.2 System Design	25
		4.2.3 Module Development	25
		4.2.4 Integration and Testing	25
		4.2.5 Validation and Deployment	25
	4.3	**Modules Discussion**	**26**
		4.3.1 Voter Registration and Authentication	26
		4.3.2 Campaign Management	26
		4.3.3 Vote Casting	26
		4.3.4 Result Management	26
		4.3.5 Blockchain Interaction	26
		4.3.6 Frontend Interface	27

	4.4	**UML Diagram**	**27**
	4.4.1	Voter Login and Authentication	27
	4.4.2	Vote Casting Process	27
	4.4.3	Sequence Diagram 4.4.4 Context Diagram	28
5	**SYSTEM IMPLEMENTATION**		**30**
	5.1	**Frontend (Node.js, HTML, CSS, JavaScript)**	**30**
	5.1.1	User Registration and Authentication	30
	5.1.2	Voting Process	31
	5.1.3	Real-Time Updates and Confirmation	32
	5.1.4	Admin Tools	32
	5.1.5	TECHNOLOGIES USED	33
	5.2	**Backend (Python API)**	**33**
	5.2.1	User Registration and Authentication	33
	5.2.2	Vote Management	34
	5.2.3	Campaign Management	34
	5.2.4	Database Operations	34
	5.2.5	API Endpoints	34
	5.2.6	Security Measures:	35
	5.3	**Blockchain Interaction (Web3, Truffle)**	**35**
	5.3.1	Smart Contracts	35
	5.3.2	Web3 Integration	35
	5.3.3	Truffle Framework	35
	5.3.4	Workflow for Vote Submission	35
	5.3.5	Deployment Scripts and Configuration	36
6	**SYSTEM TESTING AND EVALUATION**		**38**
	6.1	**Functional Testing**	**38**
	6.1.1	Voter Registration and Authentication	38
	6.1.2	Campaign and Candidate Management	38
	6.1.3	Vote Casting	38
	6.1.4	Result Management	38
	6.1.5	Error Handling	39
	6.1.6	Security and Penetration Testing	39
	6.2	**KEY SECURITY TESTS**	**39**
	6.2.1	Authentication Security	39
	6.2.2	Blockchain Data Security	39
	6.2.3	Access Control	40
	6.2.4	Common vulnerabilities	40
	6.3	**Performance Evaluation**	**41**
	6.3.1	Load Testing	41
	6.3.2	Stress Testing	42
	6.3.3	System Reliability	42
	6.3.4	Evaluation Summary	43

7 CONCLUSION 44
7.1 Summary of Findings 44
7.1.1 Voting System That Is Decentralized and Controls Tampering 44
7.1.2 Authentication That Is Reliable and Secure 44
7.1.3 Electoral Affairs That Are Fully Ineffective and Automated 44
7.1.4 Usability and User Experience 45
7.1.5 Performance and Scalability 45
7.1.6 Security and Reliability 45
7.2 Further Work and Limitations 45
7.2.1 Private Blockchain Environment 45
7.2.2 Limited Privacy Mechanisms 46
7.2.3 Hardware Compatibility 46
7.2.4 Scalability for Large Elections 46
7.2.5 User Adoption and Education 46
7.3 Future Work Opportunities 47
7.3.1 Collaboration With Global Blockchain Networks 47
7.3.2 Enhanced Privacy Measures 47
7.3.3 Layer 2 Solution for Scalability 47
7.3.4 Better Engagement Through Mobile Devices 47
7.3.5 Integration With Local Administrative Systems 47
7.3.6 Support For Other Languages 48
7.3.7 Integration with Public Ethereum Networks 48

REFERENCES 50

APPENDICES 53