

TABLE OF CONTENTS

TITLE PAGE	i
APPROVAL PAGE BY SUPERVISORY COMMITTEE.....	ii
STATEMENT OF ORIGINALITY	iii
PREFACE.....	iii
ACKNOWLEDGEMENT	iii
TABLE OF CONTENTS	vi
LIST OF TABLES.....	ix
LIST OF FIGURES	x
LIST OF SYMBOLS AND ABBREVIATIONS.....	xi
ABSTRACT.....	xii
CHAPTER I INTRODUCTION	1
1.1 Background	1
1.2 Problem Statement	6
1.3 Research Limitations	6
1.4 Research Objectives	7
1.5 Research Originality and Contributions.....	7
1.5.1 A Multi-Dimensional Endorsement-Based Trust Model for SSI	8
1.5.2 A Zero-Knowledge-Based Privacy-Preserving Trust Verification Framework.....	8
1.5.3 An Identity-Bound Zero-Knowledge Proof Mechanism.....	8
1.5.4 Implementation and Validation Using zk-SNARKs and Smart Contracts	8
1.5.5 Comprehensive Security and Privacy Analysis	9
1.6 Research Significance	9
1.7 Organization of the Research	10
CHAPTER II LITERATURE REVIEW AND THEORETICAL FOUNDATION..	11
2.1 Literature Review.....	11
2.1.1 Trust Frameworks in Self-Sovereign Identity	11
2.1.2 Zero-Knowledge Proofs for Privacy-Preserving Trust Systems	12
2.1.3 Limitations of Existing Approaches and Research Gap	13
2.1.4 Positioning of This Research.....	15
2.2 Theoretical Foundation	15
2.2.1 Foundations of Self-Sovereign Identity.....	15
2.2.2 SSI Architecture and Digital Wallets.....	16
2.2.3 Security, Privacy, and Applications of Self-Sovereign Identity	18
2.2.4 Trust Management and Evaluation in Decentralized Systems	20
2.2.5 Trust Management in Self-Sovereign Identity Systems	22
2.2.6 Zero-Knowledge Proofs for Privacy-Preserving Decentralized Systems.....	23



2.2.7	Blockchain Technology and Smart Contracts	25
2.2.8	ZKPs in Self-Sovereign Identity and Trust Systems.....	26
2.3	Research Questions	27
2.4	Hypothesis	27
CHAPTER III RESEARCH METHODOLOGY		28
3.1	System Architecture	28
3.1.1	System Components.....	28
3.1.2	Proposed Framework Architecture	29
3.1.3	Design Rationale	31
3.2	Trust Model (Direct, Reputation, Freshness)	31
3.2.1	Direct Trust (D)	31
3.2.2	Reputation Trust (R)	31
3.2.3	Freshness Factor (F).....	32
3.2.4	Final Trust Aggregation Equation.....	32
3.2.5	Trust Decision Model and Security Integration.....	34
3.3	Zokrates Circuit Design.....	34
3.3.1	Overview of Circuit Design	34
3.3.2	Input and Witness Definition.....	35
3.3.3	Constraint Construction	36
3.3.4	Identity Binding and Circuit Security Considerations	37
3.3.5	Proof Generation and Verification Workflow.....	38
3.4	Security Model (Replay Resistance, Identity Binding).....	38
3.4.1	Overview of Security Objectives	38
3.4.2	Impersonation and Replay Attack Resistance.....	39
3.4.3	Identity Binding and Trust Manipulation Resistance.....	40
3.4.4	Zero-Knowledge Privacy Guarantees	40
3.4.5	Dataset for the Research.....	41
3.4.6	Zero-Knowledge Circuit Design and Scalability Evaluation	42
3.4.7	Implementation Overview and Technology Stack	43
3.4.8	System Workflow Implementation.....	44
3.4.9	Performance Metrics	45
3.4.10	Experimental Setup.....	46
3.4.11	Hardware and Software Configuration.....	47
3.4.12	Summary	48
CHAPTER IV RESULTS AND DISCUSSION		49
4.1	Results	49
4.1.1	Verification Accuracy Evaluation	49
4.1.2	Performance Analysis of Trust Verification	50
4.1.3	Proof Generation Time Comparison.....	51
4.1.4	On-Chain Verification Cost Analysis.....	52
4.2	Discussion.....	53
4.2.1	Experimental Evaluation Overview	53



4.2.2	Trust Evaluation Performance	54
4.2.3	Blockchain Verification Evaluation.....	55
4.2.4	Security Evaluation.....	55
4.2.5	Comparative Performance Analysis with zkSSI.....	57
4.2.6	Summary of Findings	57
4.2.7	Answering the Research Questions.....	58
CHAPTER V	CONCLUSION AND RECOMMENDATIONS	59
5.1	Conclusion	59
5.2	Recommendations.....	60
REFERENCES		61
APPENDIX		A-1
Appendix 1: Algorithms		A-1
Appendix 2: System Parameters and Datasets		A-11
Appendix 3: Screenshots from Experiments.....		A-22

LIST OF TABLES

Table 2.1	Comparative Analysis of Self-Sovereign Identity Frameworks	13
Table 3.1	Zokrates Circuit Inputs	36
Table 3.2	Circuit Configurations for Trust Verification Scalability Evaluation ...	43