

IMPLEMENTING DUAL WALLET AUTHENTICATION USING SMART CONTRACTS FOR TWO-FACTOR AUTHENTICATION

SKRIPSI



**PROGRAM STUDI ILMU KOMPUTER (S1)
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KEJURUAN
UNIVERSITAS PENDIDIKAN GANESHA**



- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSR - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile VeryDS oleh BSR
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.



- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile VeryDS oleh BSrE
- Cetak dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.



**Balai Besar
Sertifikasi
Elektronik**

SKRIPSI

DIAJUKAN UNTUK MELENGKAPI TUGAS DAN MEMENUHI SYARAT-SYARAT UNTUK MENCAPAI GELAR SARJANA KOMPUTER

Menyetujui

Pembimbing I	I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs. NIP.198910262019031004
Pembimbing II	Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D. NIP.197803242005011001

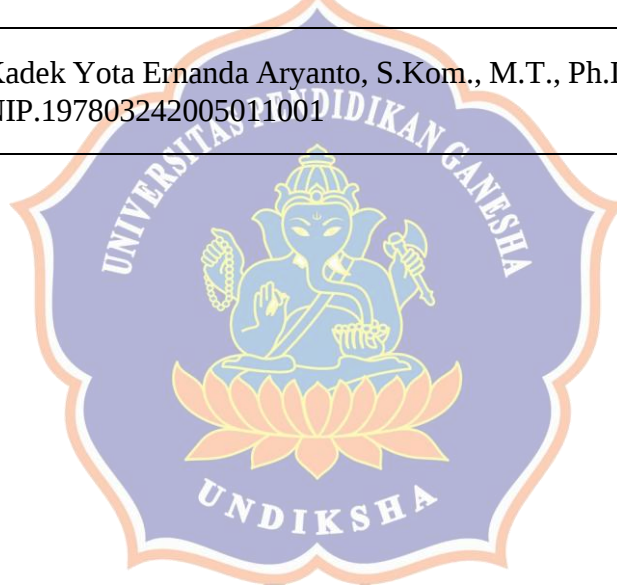


- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile VeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

Skripsi oleh Chiko Gita Satria ini
telah dipertahankan di depan dewan penguji
Pada tanggal 05 Januari 2026

Dewan Penguji

Ketua	I Ketut Purnamawan, S.Kom., M.Kom. NIP.197905112006041004
Anggota	Ir. Ketut Agus Seputra, S.ST.,M.T. NIP.199008152019031018
Anggota	I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs. NIP.198910262019031004
Anggota	Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D. NIP.197803242005011001



- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile VeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

Diterima oleh Panitia Ujian Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
guna memenuhi syarat-syarat untuk mencapai gelar Sarjana Komputer

Menyetujui

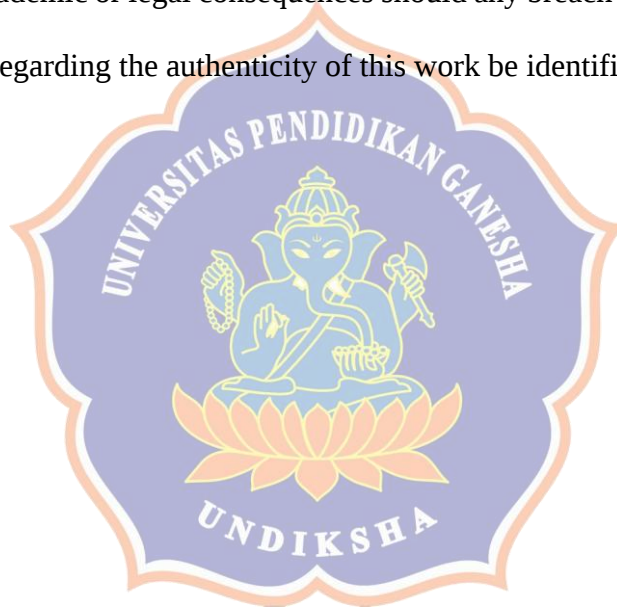
Ketua Ujian	Made Windu Antara Kesiman, S.T., M.Sc., Ph.D. NIP.198211112008121001
Sekretaris Ujian	I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs. NIP.198910262019031004



- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile VeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

DECLARATION

I hereby declare that the work entitled **<Implementing Dual Wallet Authentication Using Smart Contracts for Two-Factor Authentication>** is entirely my own original research and has been prepared without any form of plagiarism or unethical citation practices that contravene accepted academic standards. I further acknowledge that I bear full responsibility and am willing to accept any academic or legal consequences should any breach of scientific integrity or questions regarding the authenticity of this work be identified in the future.



Singaraja, January 5 2026

Writer of the thesis



A handwritten signature in black ink, appearing to be "Chiko Gita Satria".

Chiko Gita Satria
NIM 2215101053

PREFACE

First and foremost, the author would like to express gratitude to God Almighty for His blessings and guidance, which made it possible to complete this thesis entitled **<Implementing Dual Wallet Authentication Using Smart Contracts for Two-Factor Authentication.>** This thesis is submitted as a partial fulfillment of the requirements for obtaining a Bachelor's degree in Computer Science in the Computer Science Study Program, Faculty of Engineering and Vocational, Universitas Pendidikan Ganesha.

The author acknowledges that the successful completion of this thesis would not have been possible without the support, guidance, and encouragement of many individuals. In completing this thesis, the author received extensive support, both moral and material, from various parties. Therefore, the author would like to express sincere gratitude to:

1. Prof. Dr. I Wayan Lasmawan, M.Pd., as Ganesha University of Education Rector, for providing academic facilities and an environment that supports learning and research at Universitas Pendidikan Ganesha.
2. Dr. Kadek Rihendra Dantes, S.T., M.T., Dean of the Faculty of Engineering and Vocational, for administrative support and academic guidance throughout the study period.
3. Dr. Putu Hendra Suputra, S.Kom., M.Cs., Head of the Computer Science Study Program, for guidance, academic direction, and support during the completion of this thesis.
4. I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs., Thesis Supervisor I, for invaluable guidance, patience, constructive feedback, and continuous motivation throughout the research process.
5. Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D. Thesis Supervisor II, for insightful suggestions, technical direction, and support in refining this research.

6. All Board of Examiners, for their valuable comments, critiques, and recommendations that contributed to the improvement of this thesis.
7. All Lecturers of the Computer Science Study Program, for the knowledge, guidance, and inspiration provided during the author's academic journey.
8. Every one of my family members, especially My Mother Ina Noviani, My Aunt Rika Monika for all of their moral support, encouragement, financial support, and prayers throughout the completion of this study.
9. Friends and Colleagues, for their assistance, discussions, and moral support during both the research and writing phases of this thesis.
10. Other Supporting Parties, whose contributions, either directly or indirectly, have supported the successful completion of this research.

The author fully acknowledges that this thesis is far from perfect due to the limitations of the author's knowledge and experience. Therefore, constructive criticism and suggestions from various parties are highly welcomed in order to improve the quality of this thesis. The author sincerely hopes that this research may provide benefits and contribute positively, particularly to the development of education and the advancement of knowledge in the field of computer science.

Singaraja, January 5 2026

Author

Chiko Gita Satria

TABLE OF CONTENTS

Content	Page
ABSTRAK	ix
ABSTRACT	x
PREFACE	i
TABLE OF CONTENTS	iii
LIST OF FIGURES	vii
LIST OF TABLES	ix
LIST OF APPENDICES.....	x
CHAPTER I INTRODUCTION.....	1
1.1 Background.....	1
1.2 Problem Identification.....	4
1.3 Research Questions.....	4
1.4 Scope of the Study.....	5
1.5 Research Objectives.....	5
1.6 Research Significance.....	6
1.6.1 Theoretical Significance.....	6
1.6.2 Practical Significance	6
CHAPTER II LITERATURE REVIEW	7
2.1 Related Work	7
2.2 Theoretical Review	18
2.2.1 Two Factor Authentication (2FA)	18
2.2.2 Blockchain Technology and Ethereum	21
2.2.3 Wallet Concept	24
2.2.4 Smart Contracts in Digital Security	25

2.2.5	Solidity: A Programming Language for Smart Contracts	25
2.2.6	Remix IDE: Smart Contract Development Environment	25
2.2.7	Smart Contract Integration in Authentication System.....	26
2.2.8	Ethereum Testnet (Sepolia) as a Testing Environment	26
2.2.9	Node.js and React: Web Development Frameworks for 2FA Integration	27
2.2.10	Cryptographic Fundamentals in Dual Wallet-Based Authentication 28	
2.2.11	Wallet Authentication Workflow with Dual Signatures.....	29
2.3	Framework of Thinking	30
2.3.1	The problem.....	31
2.3.2	Solution Approach.....	32
2.3.3	Research Implementation	33
2.3.4	Expected results.....	33
CHAPTER III RESEARCH METHODOLOGY		34
3.1	Research Time and Place	34
3.2	Research Methods.....	35
3.3	Research Variables.....	37
3.4	Data Collection Instruments	38
3.5	Research Stages	40
3.6	Data Analysis Techniques.....	52
3.7	Research Expectations	54
CHAPTER IV RESULT AND DISCUSSION.....		55
4.1	Smart Contract Development.....	55
4.1.1	Smart Contract Logic and Features	55

4.1.2	Deployment on Sepolia Testnet.....	57
4.1.3	Smart Contract Code Summary.....	57
4.2	System Integration	58
4.2.1	Backend with Node.js and Web3.js.....	58
4.2.2	Frontend with React.....	64
4.2.3	Data and Interaction Flow	67
4.3	Smart Contract Security Testing: Necessity and Uniqueness in Dual Wallet Systems	68
4.3.1	Fuzz and Static Testing for Smart Contracts	68
4.3.2	Uniqueness to Dual Wallet Systems vs. Traditional OTP.....	70
4.3.3	The Necessity of Fuzz and Static Testing	73
4.4	Smart Contract Security Testing Results	73
4.4.1	Static Analysis with Slither	74
4.4.2	Fuzz Testing with Echidna	75
4.4.3	Summary of Detected Issues	77
4.5	Attack Simulation Results (Traditional vs. Dual Wallet)	79
4.5.1	Phishing Simulation.....	79
4.5.2	MITM (Man-in-the-Middle) Attack Simulation.....	82
4.5.3	Replay Attack Simulation and Nonce Enforcement.....	83
4.5.4	Summary of Findings	87
4.6	Evaluation of Testing Outcomes.....	91
4.6.1	Authentication Time and Cost.....	91
4.6.2	Vulnerability Density	97
4.6.3	Summary of Key Metrics.....	98
4.7	Comparative Discussion	99

4.7.1	Security Comparison	99
4.7.2	Performance and Usability Comparison	101
4.7.3	Summary of Differences	102
4.8	Additional Security and Deployment Considerations.....	104
4.8.1	Threats from Brute-Force Attacks on Nonce or Challenge Messages 104	
4.8.2	Recovery Scenario if the User Loses Access	105
4.8.3	Security Risks When Managed by a Third Party	105
4.8.4	Operation on Ethereum Mainnet with High Cost.....	106
4.8.5	Interoperability	106
4.8.6	UI/UX and Deployment Considerations	106
4.8.7	Legal and Privacy Implications	107
4.8.8	Pros and Cons of Using a Dual Wallet System	107
CHAPTER V CONCLUSION AND SUGGESTIONS.....		109
5.1	Conclusion	109
5.2	Suggestions	112
Bibliography		115
APPENDICES		121
BIOGRAPHY		132

LIST OF FIGURES

Figure 2.1 Simplified Diagram of How Blockchain Works	22
Figure 2.2 Shows How Blocks are Connected	23
Figure 2.3 Altering the Data in Blockchain.....	23
Figure 2.4 Framework of Thinking	31
Figure 3.1 Research Stages.....	41
Figure 3.2 Traditional 2FA Mechanism	43
Figure 3.3 Dual wallet-based 2FA Login Mechanism.....	46
Figure 3.4 Dual Wallet-based 2FA Registration Mechanism	47
Figure 3.5 Data Exchange in Dual Wallet-based Authentication	49
Figure 3.6 Registration and Wallet Setup Flow.....	51
Figure 4.1 Flow of Api Register.....	60
Figure 4.2 Flow of Api Login.....	61
Figure 4.3 Flow of Api Save Wallets	62
Figure 4.4 Flow of Api Get Challenge Message	62
Figure 4.5 Flow of Api Nonce Generator.....	63
Figure 4.6 Flow of Entire 2fa Api Verification	64
Figure 4.7 LoginPage Component.....	65
Figure 4.8 RegisterPage Component	66
Figure 4.9 SetupWalletsPage Component	66
Figure 4.10 TwoFactorAuthApp Component.....	67
Figure 4.11 Slither Static Analysis Result.....	75
Figure 4.12 Echidna Fuzz Testing Result.....	76
Figure 4.13 Phishing Website That Mimics the Dual Wallet	80
Figure 4.14 Phishing Website That Mimics Google Auth	81
Figure 4.15 MITM Testing Using Wireshark for Dual Wallet	82
Figure 4.16 MITM Testing Using Wireshark for Google Auth.....	83
Figure 4.17 Rejected Signature by System if Signature Already Used.....	85
Figure 4.18 Replay Attacks Using the Same OTP Code First Time	86

Figure 4.19 Replay Attacks Using the Same OTP Code Second Time.....	86
Figure 4.20 Transaction Details on Sepolia Testnet.....	94
Figure 4.21 Average time required for a user to complete authentication.....	96
Figure 4.22 compares the initial setup cost of both systems, measured in USD based on current Ethereum gas fees.	97



LIST OF TABLES

Table 2.1 Comparison between OTP-SMS Blockchain-Based 2FA Framework .	16
Table 2.2 Comparison Between Traditional Two-Factor Authentication (2FA) ..	19
Table 2.3 Comparison Using Secondary Wallet and Nonce Mechanism.....	20
Table 3.1 Research Timeline	34
Table 3.2 Tools and Methods for Data Collection in Security Testing	39
Table 3.3 Comparison of Output Metrics	53
Table 4.1 Smart Contract Deployment Summary	58
Table 4.2 System Integration Stack.....	67
Table 4.3 Slither Static Analysis Result	78
Table 4.4 Echidna Fuzz Testing Results	78
Table 4.5 Attack Possibilities in Traditional OTP Systems	88
Table 4.6 Attack Possibilities in Dual-Wallet Systems.....	89
Table 4.7 Attack Vector Comparison: Traditional OTP vs. Dual Wallet.....	89
Table 4.8 Performance and Efficiency Metrics	98
Table 4.9 Security Comparison Summary.....	101
Table 4.10 Security and Performance Comparison 3 Dual Wallet vs Traditional OTP 2FA	103
Table 4.11 Pros and Cons of the Dual Wallet-Based 2FA System	107

LIST OF APPENDICES

Appendix 1. Smart Contract User Struct Code.....	122
Appendix 2. Smart Contract registerSecondaryWallet Function Code	122
Appendix 3. Smart Contract authenticate Function Code	122
Appendix 4. Backend Database and Contract Configuration Code	123
Appendix 5. Backend Registration Route Code.....	123
Appendix 6. Backend Login Route Code.....	124
Appendix 7. Backend Save Wallets Route.....	125
Appendix 8. Backend Challenge Message Route Pseudocode.....	125
Appendix 9. Backend Nonce Generation Route.....	126
Appendix 10. Backend 2FA Verification Route.....	126
Appendix 11. Frontend App Component State Management and Navigation	127
Appendix 12. Frontend LoginPage Component Pseudocode.....	127
Appendix 13. Frontend RegisterPage Component Pseudocode	128
Appendix 14. Frontend SetupWalletsPage Component	129
Appendix 15. Frontend TwoFactorAuthApp Component	130

