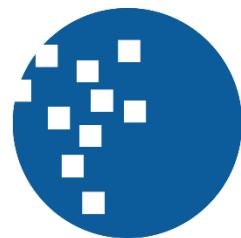


**RANCANG BANGUN SISTEM AKSES KONTROL
ELEKTRONIK BERBASIS BLOCKCHAIN**



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

Tugas Akhir

**Julando Omar
00000027458**

**PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2022**

RANCANG BANGUN SISTEM AKSES KONTROL ELEKTRONIK BERBASIS BLOCKCHAIN



Diajukan sebagai Salah Satu Syarat untuk Memperoleh
Gelar Sarjana Teknik

Julando Omar
00000027458

PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2022

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama : Julando Omar

Nomor Induk Mahasiswa : 00000027458

Program studi : Teknik Komputer

Tugas Akhir dengan judul:

RANCANG BANGUN SISTEM AKSES KONTROL
ELEKTRONIK BERBASIS BLOCKCHAIN

merupakan hasil karya saya sendiri bukan plagiat dari karya ilmiah yang ditulis oleh orang lain, dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk Tugas Akhir yang telah saya tempuh.

Tangerang, 21 Juni 2022




(Julando Omar)

UNIVERSITAS
MULTIMEDIA
NUSANTARA

HALAMAN PERSETUJUAN

Tugas Akhir dengan judul

RANCANG BANGUN SISTEM AKSES KONTROL ELEKTRONIK BERBASIS BLOCKCHAIN

Oleh

Nama : Julando Omar

NIM : 00000027458

Program Studi : Teknik Komputer

Fakultas : Teknik dan Informatika

Telah disetujui untuk diajukan pada

Sidang Ujian Tugas Akhir Universitas Multimedia Nusantara

Tangerang, 13 Juni 2022

Pembimbing


Samuel Hutagalung, M.T.I.
0304038902

Ketua Program Studi Teknik
Komputer


Samuel Hutagalung, M.T.I.

**UNIVERSITAS
MULTIMEDIA
NUSANTARA**

HALAMAN PENGESAHAN

Tugas Akhir dengan judul

RANCANG BANGUN SISTEM AKSES KONTROL ELEKTRONIK BERBASIS BLOCKCHAIN

Oleh

Nama : Julando Omar

NIM : 00000027458

Program Studi : Teknik Komputer

Fakultas : Teknik dan Informatika

Telah diujikan pada hari selasa, 21 Juni 2022

Pukul 08.00 s.d 10.00 dan dinyatakan

LULUS

Dengan susunan penguji sebagai berikut.

Ketua Sidang

Nabila Husna Shabrina, S.T.,
M.T.
0321099301

Penguji

Dareen Kusuma Halim, S.Kom.,
M.Eng.Sc.
0317129202

Pembimbing

Samuel Hutagalung, M.T.I.
0304038902

Ketua Teknik Komputer

Samuel Hutagalung, M.T.I.

UNIVERSITAS
MULTIMEDIA
NUSANTARA

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas academica Universitas Multimedia Nusantara, saya yang bertanda tangan di bawah ini:

Nama : Julando Omar
NIM : 00000027458
Program Studi : Teknik Komputer
Fakultas : Teknik dan Informatika
Jenis Karya : *Tesis/Skripsi/Tugas Akhir (*coret salah satu)

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Multimedia Nusantara Hak Bebas Royalti Nonekslusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul.

RANCANG BANGUN SISTEM AKSES KONTROL
ELEKTRONIK BERBASIS BLOCKCHAIN

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Nonekslusif ini, Universitas Multimedia Nusantara berhak menyimpan, mengalihmediakan/mengalihformatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Tangerang, 13 Juni 2022

Yang menyatakan,


UNIVERSITAS *Julando*
MULTIMEDIA
NUSANTARA
(Julando Omar)

KATA PENGANTAR-

Puji dan syukur kepada Tuhan Yang Maha Esa penulis panjatkan atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan tugas akhir dengan judul “RANCANG BANGUN SISTEM AKSES KONTROL ELEKTRONIK BERBASIS BLOCKCHAIN”.

Tugas akhir ini tidak dapat terselesaikan tanpa adanya dukungan dari berbagai pihak yang telah mendukung dan membimbing penulis. Oleh karena itu penulis ingin menyampaikan terima kasih kepada:

1. Dr. Ninok Leksono, M.A., selaku Rektor Universitas Multimedia Nusantara.
2. Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Universitas Multimedia Nusantara.
3. Samuel Hutagalung, M.T.I selaku Ketua Program Studi Teknik Komputer Multimedia Nusantara dan Dosen pembimbing tugas akhir penulis, yang menerima penulis dengan baik untuk berkonsultasi, dan memberikan bimbingan kepada penulis mengenai pembuatan dan penggerjaan tugas akhir dan tata cara penulisan karya ilmiah yang benar.
4. Keluarga saya, yaitu papa dan mama, cece Desvia dan cece Maytiska yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan tugas akhir ini.
5. Dominique Nadia, yang bersama-sama berjuang dan menyemangati untuk menyelesaikan tugas akhir.
6. Arsheldy Alvin, Aurelius Ryo Wang, Axel Patria, Edgar Christian dan Harvard Harsono yang telah menemani selama pembuatan tugas akhir.
7. Anggota Pemuda MRII GS dan GRII BSD, yang telah membantu dalam memberikan dukungan dan doa.
8. Teman-teman Teknik Komputer Angkatan 2018, yang telah Bersama-sama belajar dan berjuang untuk menyelesaikan Pendidikan strata satu,

9. Dan pihak-pihak lainnya yang tidak dapat disebutkan satu persatu yang telah membantu dalam pembuatan tugas akhir.

Akhir kata, semoga tugas akhir ini dapat bermanfaat bagi pembaca dan dapat menjadi acuan dalam penelitian-penelitian lainnya.

Tangerang, 13 Juni 2022



(Julando Omar)



RANCANG BANGUN SISTEM AKSES KONTROL ELEKTRONIK BERBASIS BLOCKCHAIN

(Julando Omar)

ABSTRAK

Sistem akses kontrol merupakan salah satu faktor yang penting dalam keamanan. Sistem akses kontrol elektronik merupakan sistem akses kontrol yang paling umum digunakan pada masa kini. Sistem akses kontrol elektronik memiliki beberapa kelebihan namun juga memiliki beberapa kekurangan seperti *single point of failure* serta adanya *log-tampering*. Hal ini dapat terjadi karena sistem akses kontrol elektronik masih menggunakan sistem yang tersentralisasi atau *centralized system*. Dengan adanya permasalahan tersebut penulis membuat solusi berupa sistem akses kontrol elektronik berbasis *blockchain*. Sistem akses kontrol elektronik menggunakan *blockchain* sendiri terdiri dari 3 bagian yaitu Frontend, Blockchain dan Node. Bagian Frontend merupakan bagian interaksi antara pengguna dengan sistem dan dibuat menggunakan bahasa pemrograman *Javascript* dan *framework Vue*. Sistem *blockchain* merupakan sistem terdistribusi yang menyimpan data sehingga data menjadi terdistribusi dan terbebas dari *log-tampering*. Sistem *blockchain* dibuat dengan menggunakan program Geth dan IPFS. Sistem Node merupakan sistem yang memberikan akses kepada pengguna. Sistem Node dibuat menggunakan Raspberry Pi dan dengan menggunakan bahasa pemrograman Python. Setelah dilakukan implementasi dan pengujian, maka didapatkan bahwa sistem dapat digunakan sebagai sistem akses elektronik yang dapat menanggulangi *single point of failure* dan memiliki *availability* yang tinggi serta dapat menanggulangi *log-tampering*. Sistem menggunakan waktu rata-rata sebanyak 35 dan 41 detik untuk memberikan akses kepada *user*. Pada pengujian sistem, juga didapatkan hasil bahwa sistem *blockchain* dengan konsensus PoW dapat digunakan pada sistem yang memiliki jumlah *node* yang banyak, sedangkan konsensus PoA dapat digunakan pada sistem yang memiliki jumlah *node* yang sedikit

Kata kunci: Blockchain, Sistem akses kontrol elektronik, IPFS, sistem terdistribusi,

UNIVERSITAS
MULTIMEDIA
NUSANTARA

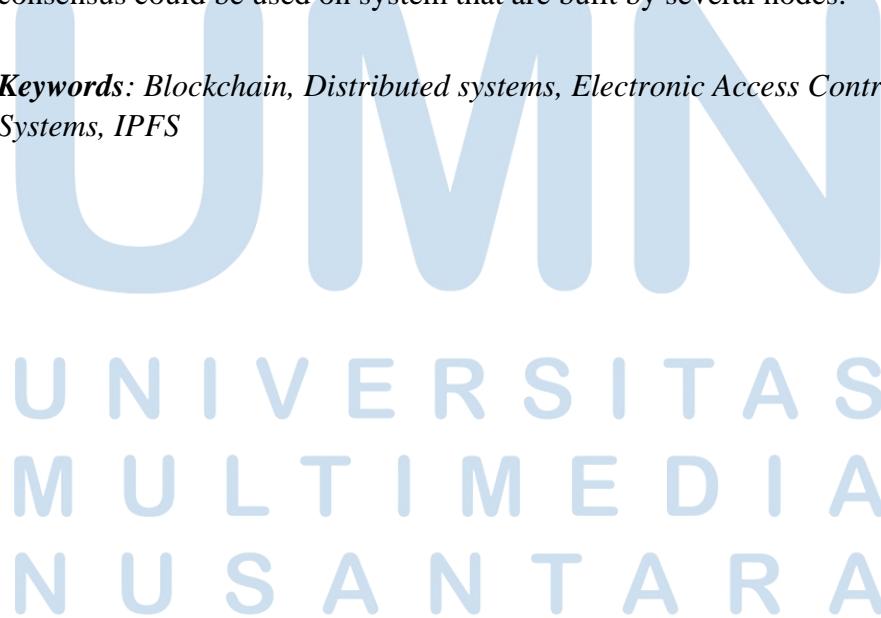
ACCESS CONTROL SYSTEM BASED ON BLOCKCHAIN

(Julando Omar)

ABSTRACT

Access control system is one of the important factors in security system. Electronic access control system is one of the popular access controls which are used today. Electronic access control system has several advantages and also have several weaknesses. These weaknesses are single point of failure and log tampering. Centralized system is the cause of these weaknesses. Based on these problems, electronic access control based on blockchain is made to solve these problems. This solution consist of three part which are Frontend, Blockchain and Node. Frontend system is the interaction point between user and the system itself. Frontend system is made using Javascript and Vue Framework. Blockchain system is a distributed system that stores data which made the system free from single point of failure and log tampering problems. Blockchain system is consist of Geth and IPFS programs. Node system is the system which gave access to users. Node system is made using Raspberry pi and Python programming language. After implementation and testing phase is done, the systems can be used as a electronic access control systems which could mitigate single point of failure with high availability and log tampering. On Average, system used 35 seconds and 41 seconds to give access to users. Blockchain with PoW consensus could be used on systems that are built by a lot of nodes, and PoA consensus could be used on system that are built by several nodes.

Keywords: *Blockchain, Distributed systems, Electronic Access Control Systems, IPFS*



DAFTAR ISI

HALAMAN PERNYATAAN TIDAK PLAGIAT	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS	v
KATA PENGANTAR-	vi
ABSTRAK	viii
ABSTRACT	ix
DAFTAR ISI.....	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR.....	xiv
DAFTAR LAMPIRAN	xviii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	5
1.6 Sistematika Penelitian.....	5
BAB II TINJAUAN PUSTAKA.....	7
2.1 Penelitian Terdahulu.....	7
2.1.1 Blockchain Based Smart Door Lock System [11]	7
2.1.2 Physical Access Control Management System Based on Permissioned Blockchain [12].....	8
2.1.3 Blockchain-based Secure Data Storage for Door Lock System [13]	10
2.1.4 IoT and Blockchain for Smart Locks [14]	11
2.1.5 Using Blockchain for Electronic Health Records [15].....	13
2.1.6 Residential access control system using QR code and the IoT [16] 14	
2.1.7 Development of Web-Based Smart Security Door Using QR Code System [17].....	15

2.1.8 Securing Face Recognition System Using Blockchain Technology [18]	17
2.1.9 FaceHub: Facial Recognition Data Management in Blockchain [19]	18
2.2 Tinjauan Teori	18
2.2.1 Blockchain	18
2.2.2 Face Recognition	21
2.2.3 Electronic Access Control	23
2.2.4 Raspberry Pi	23
2.2.5 Smart Contract	24
2.2.6 QR Code [39]	25
2.2.7 IPFS [41]	26
2.2.8 Multi Factor Authentication	27
2.2.9 Apache Cassandra [45]	28
2.2.10 BigChainDB [46]	28
2.3 Summary	29
BAB III ANALISIS DAN PERANCANGAN SISTEM	33
3.1 Metode Penelitian	33
3.2 Perancangan Modul	33
3.3 Rancangan Aplikasi	34
3.4 Rancangan Blockchain	43
3.5 Rancangan Node	46
3.6 Rancangan Deployment	52
3.7 Use Case Sistem	53
3.7.1 Admin Membuat Akun Baru	53
3.7.2 Admin Mengganti Detail User	54
3.7.3 Admin Melakukan Reset Password User	54
3.7.4 Admin Melihat Log	55
3.7.5 User Melakukan Akses	55
3.7.6 User Melihat Log Dari User	55
3.7.7 User Mengganti Password	56
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM	57
4.1 Spesifikasi Sistem	57

4.2 Implementasi Sistem	58
4.2.1 Implementasi Frontend	58
4.2.2 Implementasi Blockchain	79
4.2.3 Implementasi Node	100
4.2.4 Implementasi Deployment	112
4.3 Hasil Pengujian Sistem	117
4.3.1 Pengujian Performa.....	118
4.3.2 Pengujian Log Tampering	121
4.3.3 Pengujian Availability	132
4.4 Analisis Hasil Pengujian Sistem.....	136
4.4.1 Analisis Hasil Pengujian Performa	136
4.4.2 Analisis Hasil Pengujian Log-Tampering.....	138
4.4.3 Analisis Hasil Pengujian Availability.....	140
4.5 Kendala dan Solusi.....	142
BAB V SIMPULAN DAN SARAN	144
5.1 Simpulan.....	144
5.2 Saran.....	145
DAFTAR PUSTAKA	146
LAMPIRAN.....	150



DAFTAR TABEL

Tabel 4.1 Hasil Pengujian performa menggunakan konsensus PoW Ethash.....	120
Tabel 4.2 Hasil pengujian performa menggunakan konsensus PoA Clique	121
Tabel 4.3 Hasil pengujian <i>avaibility</i> dengan 2 <i>node</i> pada konsensus PoW Ethash	133
Tabel 4.4 Hasil pengujian <i>avaibility</i> dengan 2 <i>node</i> pada konsensus PoA Clique	134
Tabel 4.5 Hasil pengujian <i>avaibility</i> dengan 1 <i>node</i> pada konsensus PoW Ethash	135



DAFTAR GAMBAR

Gambar 2.1 Diagram use case.....	12
Gambar 2.2 Arsitektur sistem	12
Gambar 2.3 Cara kerja sistem	13
Gambar 2.4 Alur sistem kerja penelitian [17].....	16
Gambar 2.5 Cara kerja pengenal wajah metode deep learning.....	22
Gambar 2.6 Raspberry Pi 4 Model B [36]	24
Gambar 2.7 QR Code	25
Gambar 2.8 Diagram state of the art	31
Gambar 3.1 Rancangan Modul	34
Gambar 3.2 Arsitektur sistem Frontend	35
Gambar 3.3 Flow Aplikasi Frontend.....	36
Gambar 3.4 Desain laman login.....	36
Gambar 3.5 Desain laman admin	38
Gambar 3.6 Laman manage user.....	39
Gambar 3.7 Laman add user	40
Gambar 3.8 Laman log.....	41
Gambar 3.9 Laman user	42
Gambar 3.10 Laman user saat menunjukan QR Code	42
Gambar 3.11 Laman user untuk mengganti password.....	43
Gambar 3.12 Arsitektur sistem Blockchain	44
Gambar 3.13 Arsitektur penyimpanan data log dan data user	46
Gambar 3.14 Flow sistem Node.....	47
Gambar 3.15 Laman home.....	48
Gambar 3.16 Laman QR Code.....	49
Gambar 3.17 Laman face recognition.....	50
Gambar 3.18 Laman loading.....	51
Gambar 3.19 hardware diagram node	52
Gambar 3.20 Alur deployment smart contract.....	52
Gambar 3.21 Use Case ketika admin membuat user baru	53
Gambar 3.22 Use Case ketika <i>admin</i> melakukan <i>update user</i>	54
Gambar 3.23 Use case ketika <i>admin</i> melakukan <i>update password user</i>	54
Gambar 3.24 Use Case admin melihat log.....	55
Gambar 3.25 Use case <i>user</i> melakukan akses	55
Gambar 3.26 Use case <i>user</i> melihat log dari user	55
Gambar 3.27 Use case <i>user</i> mengganti <i>password</i>	56
Gambar 4.1 Struktur sistem frontend	59
Gambar 4.2 Tampilan laman login	61
Gambar 4.3 fungsi “connectToBlockchain”	61
Gambar 4.4 fungsi “isAdminRole” yang digunakan untuk mendapatkan role serta menyimpan cookies “role”.....	61
Gambar 4.5 hamburger menu pada header	62

Gambar 4.6 Navigation bar admin	62
Gambar 4.7 Navigation bar user	63
Gambar 4.8 Tampilan laman <i>admin</i>	64
Gambar 4.9 Fungsi untuk mengambil jumlah <i>user</i> dan mengambil 3 <i>log</i> teratas.	65
Gambar 4.10 Fungsi untuk mendapatkan <i>page</i> dan <i>user</i>	66
Gambar 4.11 Fungsi “ <i>disableUser</i> ”	66
Gambar 4.12 Fungsi “ <i>enableUser</i> ”	67
Gambar 4.13 Tampilan laman <i>manage user</i>	67
Gambar 4.14 Tampilan <i>dropdown user</i>	68
Gambar 4.15 Tampilan <i>dropzone user</i>	69
Gambar 4.16 Tampilan <i>modal add user</i>	70
Gambar 4.17 Fungsi untuk menyimpan <i>user</i>	71
Gambar 4.18 Fungsi “ <i>resetPassword</i> ”	72
Gambar 4.19 Tampilan laman <i>admin log</i>	73
Gambar 4.20 Tampilan apabila status <i>log</i> bukan merupakan “allowed”	73
Gambar 4.21 Fungsi “ <i>getLog</i> ”	74
Gambar 4.22 Tampilan Laman <i>user</i>	75
Gambar 4.23 Tampilan User pada saat <i>user</i> menekan tombol “Get Private Key”	76
Gambar 4.24 Fungsi untuk mendapatkan <i>QR Code</i>	76
Gambar 4.25 Tampilan laman <i>user</i> ketika sistem berhasil menampilkan <i>QR Code</i>	77
Gambar 4.26 Fungsi untuk mengubah <i>password</i>	78
Gambar 4.27 Tampilan untuk merubah <i>password</i>	79
Gambar 4.28 Tampilan <i>log user</i>	79
Gambar 4.29 <i>command</i> untuk melakukan instalasi <i>geth</i>	80
Gambar 4.30 Pembuatan akun pada konsensus PoW	81
Gambar 4.31 Pembuatan akun pada konsensus PoA	81
Gambar 4.32 Konfigurasi <i>genesis block</i> untuk konsensus Ethash	83
Gambar 4.33 Konfigurasi <i>genesis block</i> untuk konsensus Clique	84
Gambar 4.34 Konfigurasi untuk melakukan ekspor file <i>genesis block</i> pada konsensus Ethash	85
Gambar 4.35 Konfigurasi untuk melakukan ekspor file <i>genesis block</i> pada konsensus clique	85
Gambar 4.36 <i>Command</i> “ <i>scp</i> ” untuk meng- <i>copy</i> file <i>genesis</i>	85
Gambar 4.37 <i>Command</i> untuk membuat <i>key</i> dan menjalankan <i>bootnode</i>	86
Gambar 4.38 Konfigurasi <i>genesis</i> untuk konsensus PoW	87
Gambar 4.39 Konfigurasi <i>genesis</i> untuk konsensus PoA	87
Gambar 4.40 Tampilan <i>geth</i> pada konsensus PoW pada saat jaringan <i>blockchain</i> dijalankan	89
Gambar 4.41 Tampilan <i>geth</i> pada konsensus PoW pada saat jaringan <i>blockchain</i> dijalankan	91
Gambar 4.42 <i>log</i> dari <i>geth</i> yang melakukan <i>mining block</i>	92

Gambar 4.43 Hasil <i>command</i> “geth attach --exec “admin.peers”” pada ketiga <i>node</i>	92
Gambar 4.44 Proses instalasi IPFS	93
Gambar 4.45 Proses inisialisasi IPFS, pembentukan dan penyebaran <i>swarm key</i>	94
Gambar 4.46 Proses konfigurasi <i>node-1</i> IPFS	95
Gambar 4.47 Proses konfigurasi <i>node-2</i> IPFS	96
Gambar 4.48 Proses konfigurasi <i>node-3</i> IPFS	96
Gambar 4.49 Konfigurasi <i>address listening</i> pada <i>gateway</i> IPFS	97
Gambar 4.50 Konfigurasi <i>gateway writable</i> IPFS	98
Gambar 4.51 Fungsi “safeMint” pada <i>smart contract</i> “UserToken”	99
Gambar 4.52 Fungsi “safeMint” pada <i>smart contract</i> “LogToken”	100
Gambar 4.53 File “facerecog.py”	101
Gambar 4.54 File “newUser.py”	103
Gambar 4.55 Fungsi inisialisasi pada “node.py”	105
Gambar 4.56 Fungsi “qrPage”	106
Gambar 4.57 Fungsi “log_timeout”	107
Gambar 4.58 Fungsi “allowedLog”	107
Gambar 4.59 Fungsi “createLog”	107
Gambar 4.60 Fungsi “decodeAddress”	108
Gambar 4.61 Fungsi “getPicture”	109
Gambar 4.62 Fungsi “main”	110
Gambar 4.63 Laman <i>home</i>	110
Gambar 4.64 Laman <i>scan QR</i>	111
Gambar 4.65 Laman <i>loading</i>	112
Gambar 4.66 Laman <i>face recognition</i>	112
Gambar 4.67 Konfigurasi <i>load balancer</i>	113
Gambar 4.68 Diagram <i>Script deployment smart contract</i>	115
Gambar 4.69 Hasil menjalankan <i>script deployment</i>	115
Gambar 4.70 Pembuatan IPNS	116
Gambar 4.71 Hasil <i>command</i> “npm run build”	116
Gambar 4.72 Hasil dari <i>command</i> untuk melakukan <i>hosting</i> Frontend	117
Gambar 4.73 Hasil dari <i>command</i> “scp” pada Node	117
Gambar 4.74 Foto yang akan digunakan dalam pembuatan akun pengujian	119
Gambar 4.75 Alur pengujian performa menggunakan konsensus PoW	119
Gambar 4.76 Alur pengujian log tampering pada konsensus PoW dengan 1 node attacker	122
Gambar 4.77 <i>Block</i> terakhir 3 <i>node</i> terhubung	122
Gambar 4.78 <i>Log</i> waktu <i>deployment smart contract</i> dan Frontend	123
Gambar 4.79 Geth pada <i>node</i> 3 tanpa menggunakan <i>parameter</i> “bootnodes” dan dengan <i>parameter</i> “nodiscover”	123
Gambar 4.80 Perbandingan jumlah <i>block</i> sebelum ketiga <i>node</i> disambungkan kembali	124
Gambar 4.81 <i>Log</i> waktu pembuatan <i>token log</i>	124

Gambar 4.82 Deteksi <i>sidechain ghost-attack</i> pada <i>node 1</i> dan <i>node 2</i>	124
Gambar 4.83 Perbedaan jaringan <i>blockchain</i> pada <i>node 1</i> dan <i>node 2</i> dengan <i>node 3</i>	125
Gambar 4.84 Alur Pengujian log tampering dengan 2 node penyerang	126
Gambar 4.85 <i>Block</i> terakhir dimana 3 <i>node</i> masih terhubung	126
Gambar 4.86 Log waktu <i>deployment smart contract</i> dan Frontend.....	127
Gambar 4.87 Jarak antara <i>block</i> pada <i>node 1</i> dengan <i>node 2</i> dan <i>node 3</i>	127
Gambar 4.88 Tampilan <i>command geth</i> pada <i>node 1</i> tanpa <i>parameter</i> “bootnodes” dan dengan <i>parameter</i> “nodiscover”	128
Gambar 4.89 log waktu pembuatan <i>log token</i>	128
Gambar 4.90 Perbedaan laman log pada dua ip <i>node</i>	129
Gambar 4.91 Tampilan laman log setelah penggabungan node dengan IP node-2	129
Gambar 4.92 Alur pengujian log tampering pada konsensus PoA	131
Gambar 4.93 log waktu untuk <i>deployment smart contract</i> dan <i>deployment</i> Frontend	131
Gambar 4.94 <i>Block</i> terakhir pada jaringan <i>blockchain</i> gabungan	132
Gambar 4.95 <i>Block</i> terakhir yang dapat di-mine oleh <i>node 1</i>	132



DAFTAR LAMPIRAN

Lampiran A Hasil log pengujian performa konsensus PoW pada block 1-500 ..	150
Lampiran B Hasil log pengujian performa konsensus PoW pada block 500-1000 ..	150
Lampiran C Hasil log pengujian performa konsensus PoW pada block 1000 – 1500 ..	150
Lampiran D Hasil log pengujian performa konsensus PoA pada block 1 – 500	151
Lampiran E Hasil log pengujian performa konsensus PoA pada block 500 - 1000 ..	151
Lampiran F Hasil log pengujian performa konsensus PoA pada block 1000 - 1500 ..	151
Lampiran G Hasil log pengujian avaibility konsensus PoW pada node 1 dan node 2 ..	152
Lampiran H Hasil log pengujian avaibility konsensus PoW pada node 1 dan node 3 ..	152
Lampiran I Hasil log pengujian avaibility konsensus PoW pada node 1 dan node 2 ..	153
Lampiran J Hasil log pengujian avaibility konsensus PoA pada node 1 dan node 2 ..	153
Lampiran K Hasil log pengujian avaibility konsensus PoA pada node 1 dan node 3 ..	154
Lampiran L Hasil log pengujian avaibility konsensus PoW pada node 1 ..	154
Lampiran M Hasil log pengujian avaibility konsensus PoW pada node 2 ..	154
Lampiran N Hasil Turnitin ..	155

