



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

**SISTEM VOTING BERBASIS *BLOCKCHAIN*
MENGUNAKAN ALGORITMA RAFT DAN ENKRIPSI
ASIMETRIK ECDSA**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar
Sarjana Teknik**



Farell Sujanto Moh Harsin

14110210008

**PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2018**

LEMBAR PENGESAHAN SKRIPSI

SISTEM VOTING BERBASIS *BLOCKCHAIN* MENGUNAKAN ALGORITMA RAFT DAN ENKRIPSI ASIMETRIK ECDSA

Oleh

Nama : Farell Sujanto Moh Harsin

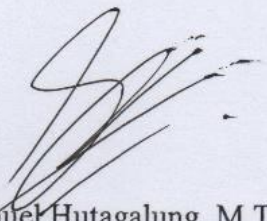
NIM : 14110210008

Fakultas : Teknik dan Informatika

Program Studi : Teknik Komputer


Tangerang, 09 Mei 2018

Ketua Sidang,



Samuel Hutagalung, M.T.I

Dosen Penguji,



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

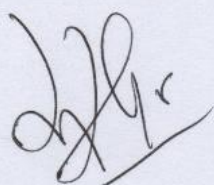
Dosen Pembimbing,



Hargyo Tri Nugroho, S.Kom., M.Sc.

Disahkan oleh,

Ketua Program Studi Sistem Komputer



Hargyo Tri Nugroho, S.Kom., M.Sc.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya,

Nama : Farell Sujanto Moh Harsin

NIM : 14110210008

Program Studi : Teknik Komputer

Fakultas : Teknik dan Informatika

Menyatakan bahwa skripsi yang berjudul “SISTEM VOTING BERBASIS *BLOCKCHAIN* MENGGUNAKAN ALGORITMA RAFT DAN ENKRIPSI ASIMETRIK ECDSA” ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya 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 mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 09 Mei 2018



Farell Sujanto Moh Harsin

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa yang selalu menyertai selama masa pengerjaan skripsi dan laporan skripsi berjudul “SISTEM VOTING BERBASIS *BLOCKCHAIN* MENGGUNAKAN ALGORITMA RAFT DAN ENKRIPSI ASIMETRIK ECDSA” sehingga dapat diselesaikan dengan baik dan benar. Skripsi ini diajukan kepada Program Studi Sistem Komputer, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara.

Penyelesaian skripsi ini juga dibantu dan didukung oleh berbagai pihak, seperti teman-teman, dosen-dosen pembimbing, dan keluarga. Oleh karena itu, ucapan terima kasih yang sebesar-besarnya diucapkan kepada:

1. Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara,
2. Hira Meidia, Ph. D., selaku Wakil Rektor Bidang Akademik dan Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara,
3. Ir. Andrey Andoko, M.Sc., selaku Wakil Rektor Bidang *Administrasi* Umum dan Keuangan,
4. Ika Yanuarti, S.E., MSF., selaku Wakil Rektor Bidang Kemahasiswaan,
5. Prof. Dr. Muliawati G. Siswanto, M.Eng.Sc., selaku Wakil Rektor Bidang Hubungan dan Kerjasama,
6. Hargyo Tri Nugroho, S.Kom., M.Sc., Ketua Program Studi Sistem Komputer Universitas Multimedia Nusantara dan dosen pembimbing pengerjaan skripsi yang selalu memberikan saran dan motivasi selama proses pengerjaan skripsi ,

7. Kedua orang tua serta adik yang selalu mendukung selama proses pengerjaan skripsi,
8. Seluruh rekan mahasiswa program studi Sistem Komputer yang telah mendukung dan membantu,

Semoga skripsi ini dapat bermanfaat bagi pembaca, baik sebagai informasi maupun sumber inspirasi, terutama untuk mahasiswa Universitas Multimedia Nusantara dalam mengembangkan teknologi informasi dan komunikasi.

Tangerang, 09 May 2018



Farell Sujanto Moh Harsin

ABSTRAKSI

Pada penelitian ini dirancang sebuah aplikasi berbasis mobile menggunakan arsitektur *blockchain* sebagai sarana penyimpanan data untuk mengurangi masalah-masalah yang ada dalam sistem yang tersentralisasi. Algoritma konsensus yang digunakan bernama Raft, dibangun dengan menggunakan framework React Native untuk diterapkan pada sistem aplikasi mobile. Menggunakan *blockchain*, sistem voting ini keaslian datanya dapat diandalkan. Pengujian menunjukkan bahwa aplikasi yang dirancang memiliki processing time yang relatif memakan waktu serta masih rentan terhadap serangan majority attack sehingga perlu penyempurnaan lebih lanjut.

Kata kunci: Raft, *blockchain*, mobile, voting, desentralisasi, database.



ABSTRACT

This research designed a mobile-based applications using blockchain architecture as a means of data storage to reduce the problems that exist in a centralized system. The consensus algorithm used, called Raft, is built using the React Native framework to be applied to mobile application systems. Using blockchain, this voting system is reliable. The test results show that the designed application has a relatively time-consuming processing time and is still vulnerable to attack attack majority so that further improvement is needed.

Keywords: Raft, *blockchain*, mobile, voting, decentralized, database.



DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI.....	ii
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	iii
KATA PENGANTAR	iv
ABSTRAKSI.....	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xiv
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	3
1.3. Tujuan Penelitian.....	3
1.4. Batasan Masalah.....	4
1.5. Manfaat Penelitian.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1. <i>Blockchain</i>	5
2.1.1. Hash.....	6
2.1.1.1 SHA-256.....	7
2.1.2. Konsensus	8
2.1.2.1 Raft.....	8
2.1.3. Asymmetric Cryptography.....	9
2.1.3.1 ECC.....	10
2.2. React Native	11
2.3. Komunikasi.....	12
2.3.1. <i>Peer-to-peer</i>	12
2.3.2. Unicast.....	12

2.3.3.	Broadcast.....	13
2.4.	Penelitian Terkait.....	14
2.4.1.	A Smart Contract for Boardroom Voting with Maximum Voter Privacy 14	
2.4.1.1	Self-Tallying Voting Protocol	14
2.4.1.2	The Open Vote Network Protocol	15
2.4.1.3	Ethereum Network.....	16
2.4.2.	Digital Voting with the use of <i>Blockchain</i> Technology.....	16
2.4.2.1	Registrasi	17
2.4.2.2	Voting	17
2.4.3.	Raft-based consensus for Ethereum/Quorum.....	19
BAB III METODE PENELITIAN.....		21
3.1.	Metode Penelitian.....	21
3.2.	Perancangan Sistem <i>Blockchain</i>	22
3.3.	Perancangan Algoritma Konsensus	24
3.3.1.	Perancangan Algoritma Raft	24
3.3.2.	Perancangan Protokol <i>Peer-to-peer</i>	28
3.4.	Perancangan Aplikasi Mobile.....	29
3.4.1.	Perancangan Sistem	29
3.4.1.1	Registrasi	29
3.4.1.2	Input Data	30
3.4.2.	Perancangan User Interface.....	31
3.4.2.1	Rancangan Halaman Login.....	31
3.4.2.2	Rancangan Halaman Register.....	32
3.4.2.3	Rancangan Menu Utama.....	33
3.4.2.4	Rancangan Halaman Home	34
3.4.2.5	Rancangan Halaman Voting	35
3.4.2.6	Rancangan Halaman View Recent Blocks	36
3.4.2.7	Rancangan Halaman Create New Vote	38
3.4.3.	Integrasi <i>Blockchain</i> dan Konsensus.....	39
3.5.	Pengumpulan Data Penelitian.....	40
3.6.	Instrumen Penelitian.....	40
BAB IV IMPLEMENTASI DAN PENGUJIAN		41

4.1.	Uji Keamanan.....	41
4.1.1.	Pengujian <i>Leader Election</i>	41
4.1.2.	Pengujian <i>Leader Election</i> Dengan <i>Majority attack</i>	43
4.1.3.	Pengujian Input Data Tanpa Anomali.....	45
4.1.4.	Pengujian Input Data Dengan <i>Majority attack</i>	46
4.1.5.	Cara Penanggulangan Majority Attack	47
4.2.	Uji Fungsionalitas.....	48
4.3.	Uji Banding dan Performa.....	58
4.3.1.	Uji Kecepatan Pencarian Data	58
4.3.2.	Uji Kecepatan Penambahan Data.....	61
4.3.3.	Simulasi Data Flooding.....	63
BAB V SIMPULAN DAN SARAN		65
5.1.	Simpulan.....	65
5.2.	Saran.....	66
DAFTAR PUSTAKA		67
LAMPIRAN I KODE PROGRAM.....		69
LAMPIRAN II FORMULIR KONSULTASI SKRIPSI.....		70



DAFTAR GAMBAR

Gambar 2.1 Grafik kurva ECC [8]	11
Gambar 2.2 Alur komunikasi unicast.....	13
Gambar 2.3 Alur komunikasi broadcast.....	13
Gambar 3.1 Block diagram alur penelitian	21
Gambar 3.2 Diagram sekuensial cara kerja sistem blockchain yang dirancang	22
Gambar 3.3 Flowchart leader election	26
Gambar 3.4 Flowchart log append	28
Gambar 3.5 Alur komunikasi <i>peer-to-peer</i>	28
Gambar 3.6 Diagram sekuensial input data	31
Gambar 3.7 Rancangan halaman login	32
Gambar 3.8 Rancangan halaman register.....	33
Gambar 3.9 Rancangan menu utama	34
Gambar 3.10 Rancangan halaman home.....	34
Gambar 3.11 Rancangan halaman voting	35
Gambar 3.12 Rancangan voting modal.....	36
Gambar 3.13 Rancangan halaman view recent blocks.....	37
Gambar 3.14 Rancangan view recent blocks modal	38
Gambar 3.15 Rancangan halaman create new vote	39
Gambar 4.1 Hasil awal <i>script</i> broker <i>peer-to-peer</i>	41
Gambar 4.2 Hasil awal <i>script</i> algoritma konsensus	42

Gambar 4.3 Hasil <i>script</i> konsensus kedua dan ketiga.....	42
Gambar 4.4 Hasil <i>script</i> konsensus setelah pemimpin terputus.....	43
Gambar 4.5 Hasil pemilihan <i>leader</i> dengan <i>majority attack</i>	44
Gambar 4.6 Hasil penambahan data.....	45
Gambar 4.7 Hasil penambahan data dengan <i>majority attack</i>	46
Gambar 4.8 Tampilan halaman Awal / Login.....	49
Gambar 4.9 Tampilan Alert bila login gagal	49
Gambar 4.10 Tampilan halaman Register.....	50
Gambar 4.11 Tampilan jika registrasi berhasil	51
Gambar 4.12 Tampilan Alert jika registrasi gagal (username sudah terdaftar)	51
Gambar 4.13 Tampilan Alert jika registrasi gagal (username invalid)	51
Gambar 4.14 Tampilan Alert jika registrasi gagal (password invalid)	51
Gambar 4.15 Tampilan Home.....	52
Gambar 4.16 Tampilan drawer menu.....	53
Gambar 4.17 Tampilan awal voting.....	54
Gambar 4.18 Tampilan Alert jika vote id belum terdaftar.....	54
Gambar 4.19 Tampilan Alert jika vote id telah mencapai batas voting.....	54
Gambar 4.20 Tampilan Alert jika pengguna telah melakukan voting pada vote id tersebut.....	54
Gambar 4.21 Tampilan Modal jika vote id valid.....	55
Gambar 4.22 Tampilan Alert konfirmasi voting.....	56

Gambar 4.23 Tampilan Alert setelah konfirmasi.....	56
Gambar 4.24 Tampilan Alert jika pengguna belum memilih kandidat.....	56
Gambar 4.25 Tampilan recent blocks	57
Gambar 4.26 Tampilan recent blocks sesuai dengan vote id	57
Gambar 4.27 Tampilan create vote	58
Gambar 4.28 Grafik waktu pencarian data	60
Gambar 4.29 Grafik waktu penambahan data.....	62
Gambar 4.30 Grafik simulasi diskret flooding.....	64



DAFTAR TABEL

Tabel 3.1 Format JSON dalam <i>blockchain</i>	23
Tabel 4.1 Kecepatan proses pencarian data	59
Tabel 4.2 Kecepatan proses penambahan data.....	62

