



INSTITUT TEKNOLOGI DEL

PEMBANGUNAN SISTEM E-VOTING MENGGUNAKAN TEKNOLOGI BLOCKCHAIN (STUDI KASUS : IT DEL)

DOKUMEN TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Diploma III

11316004 Cici Damayanti Munthe

11316013 Marchel Pirma Sakti Hutagalung

FAKULTAS INFORMATIKA DAN TEKNIK ELEKTRO

PROGRAM STUDI DIII TEKNIK INFORMATIKA

LAGUBOTI

AGUSTUS 2019

HALAMAN PERNYATAAN ORISINALITAS

HALAMAN PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya kelompok TA-D3TI04 sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah kami nyatakan dengan benar.

Nama : Cici Damayanti Munthe
NIM : 11316004
Tanda Tangan : *zlf*
Tanggal : 09 Agustus 2019

Nama : Marchel Pirma Sakti Hutagalung
NIM : 11316013
Tanda Tangan : *Mph*
Tanggal : 09 Agustus 2019

HALAMAN PENGESAHAN

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh

1. Nama : Cici Damayanti Munthe
NIM : 11316004
Program Studi : DIII Teknik Informatika

2. Nama : Marchel Pirma Sakti Hutagalung
NIM : 11316013
Program Studi : DIII Teknik Informatika

Judul Tugas Akhir : Pembangunan Sistem E-Voting Menggunakan
Teknologi Blockchain (Studi Kasus : IT DEL)

Telah berhasil dipertahankan dihadapan Dewan penguji dan diterima sebagai
bagian persyaratan yang diperlukan untuk memperoleh gelar Diploma III, pada
program studi Diploma III Teknik Informatika, Fakultas Informatika dan Teknik
Elektro, Institut Teknologi Del.

DEWAN PENGUJI:

Pembimbing : Togu Novriansyah Turnip, S.S.T., M.I.M

Penguji : Yuniarta Basani, S.Si., M.Si

Penguji : Anthon Roberto Tampubolon, S.Kom., M.T



Ditetapkan di : Laguboti
Tanggal : 09 Agustus 2019

KATA PENGANTAR

Puji dan syukur kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya penulis dapat menyelesaikan pengerjaan Tugas Akhir ini sebagaimana mestinya. Laporan Tugas Akhir ini ditulis sebagai syarat kelulusan Diploma III Institut Teknologi Del. Laporan Tugas Akhir ini bertujuan untuk mendokumentasikan hasil Tugas Akhir berjudul "***Pembangunan Sistem E-Voting Menggunakan Teknologi Blockchain (Studi Kasus : IT DEL)***".

Penyusunan Tugas Akhir ini tidak dapat diselesaikan sebagaimana mestinya tanpa bantuan dan dukungan dari berbagai pihak. Oleh kerena itu, penulis mengucapkan terimakasih yang sebesar-besarnya kepada Bapak Togu Turnip, S.S.T., M.I.M. selaku pembimbing yang telah memberikan ide, arahan, dan bimbingan, serta perbaikan selama pengerjaan Tugas Akhir ini. Penulis juga mengucapkan terimakasih yang sebesar-besarnya kepada Ibu Yuniarta Basani, S.Si,M. selaku ketua penguji dan Bapak Anthon Roberto Tampubolon, S. Kom., M.T selaku anggota penguji yang telah memberikan review dan masukan selama pengerjaan Tugas Akhir. Penulis juga berterima kasih kepada Bapak Togu Turnip, S.S.T., M.I.M dan Ibu Hernawati Susanti Samosir, SST., M. Kom selaku koordinator Tugas Akhir, dan seluruh keluarga dan teman yang telah memberikan dukungan positif kepada Penulis selama pengerjaan Tugas Akhir ini. Penulis berharap dokumen Tugas Akhir ini dapat memberikan manfaat bagi pribadi penulis, almamater, masyarakat, dan seluruh pihak yang memerlukannya demi kemajuan dan peningkatan kualitas pendidikan di masa yang akan datang.

Penulis menyadari bahwa laporan Tugas Akhir ini masih memiliki banyak kekurangan, untuk itu penulis mengharapkan saran dan kritik yang membangun untuk pengembangan dan penelitian selanjutnya.

Laguboti, 09 Agustus 2019

Penulis

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS
AKHIR UNTUK KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Institut Teknologi Del, saya yang bertanda tangan dibawah ini :

1. Nama : Cici Damayanti Munthe
NIM : 11316004
Program Studi : DIII Teknik Informatika
2. Nama : Marchel Pirma Sakti Hutagalung
NIM : 11316013
Program Studi : DIII Teknik Informatika
Fakultas : Fakultas Informatika dan Teknik Elektro
Jenis Karya : Tugas Akhir

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Institut Teknologi Del Hak Bebas *Royalty Noneksklusif (Non-exclusive Royalty-Free Right)* atas karya ilmiah kami yang berjudul:

Pembangunan Sistem E-Voting Menggunakan Teknologi Blockchain (Studi Kasus : IT DEL)

Dengan Hak Bebas Royalti Noneksklusif ini Institut Teknologi Del berhak menyimpan, mengalih/media-format dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir penulis selama tetap mencantumkan nama penulis sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini kami buat dengan sebenarnya.

Dibuat di : Laguboti
Tanggal : 09 Agustus 2019

Yang Menyatakan


(Cici Damayanti Munthe)


(Marchel Pirma Sakti Hutagalung)

ABSTRAK

Nama	:	Cici Damayanti Munthe
Program Studi	:	Diploma III Teknik Informatika
Nama	:	Marchel Hutagalung
Program Studi	:	Diploma III Teknik Informatika
Judul	:	Pembangunan Sistem E-Voting Menggunakan Teknologi Blockchain (Studi Kasus : IT DEL)

Sistem e-voting menggunakan teknologi blockchain adalah sistem elektronik untuk melakukan pemilihan dan perhitungan suara dengan menggunakan sistem terdistribusi untuk kegiatan voting. Saat ini sistem yang masih digunakan untuk melakukan voting menggunakan sistem tersentralisasi atau sistem terpusat yang menjadi pusat pengumpulan hasil voting. Terdapat beberapa permasalahan yang terjadi menggunakan sistem e-voting seperti serangan pada kerahasiaan dan keamanan data voting. Serangan yang sering terjadi pada kerahasiaan data voting adanya suatu pihak atau organisasi tertentu yang memiliki hak akses masuk ke dalam server pusat pada sistem sehingga memungkinkan pihak tersebut untuk mengetahui secara langsung identitas voter yang melakukan voting dan masing-masing hasil voting setiap voter. Sedangkan serangan yang terjadi pada keamanan data voting adalah kemungkinan untuk memodifikasi *database* voting, maka hasil perolehan voting menjadi tidak sah atau tidak valid.

Dalam Tugas Akhir ini solusi yang ditawarkan untuk mengatasi permasalahan pada sistem e-voting yang digunakan saat ini adalah menggunakan sistem terdistribusi dengan basis data yang mencatat semua transaksi voting dibagikan kepada semua pihak yang berpartisipasi atau disebut dengan Teknologi Blockchain.

Tujuan dibangunnya sistem e-voting ini adalah untuk merancang dan membangun sistem e-voting menggunakan teknologi blockchain serta membuktikan keamanan hasil data voting dalam aspek *accuracy*, *invulnerability*, *privacy*, dan *verifiability* tercapai. Untuk mempercepat proses *development* sistem e-voting digunakan salah satu API Blockchain yaitu layanan API SoChain. API SoChain adalah layanan yang digunakan untuk terhubung pada sistem e-voting untuk membuat dan mengambil transaksi voting pada testnet bitcoin berdasarkan *bitcoin address*.

Pengujian untuk sistem e-voting dilakukan dengan membuat skenario pengujian pada fungsi yang terdapat pada sistem berdasarkan *use case scenario* dan untuk pembuktian pada aspek metode keamanan yang akan dicapai dijelaskan secara naratif. Hasil dari pengujian sistem ini adalah sistem e-voting menggunakan teknologi blockchain dengan dengan aspek keamanan mencakup *accuracy*, *invulnerability*, *privacy*, dan *verifiability*.

Kata Kunci : *E-voting, Blockchain, Kerahasiaan, Keamanan, API, Accuracy, Invulnerability, Privacy, dan Verifiability*

ABSTRACT

Name	:	Cici Damayanti Munthe
Study Program	:	Diploma III Informatic Engineering
Name	:	Marchel Hutagalung
Study Program	:	Diploma III Informatic Engineering
Title	:	<i>E-Voting System Development Using Blockchain Technology (Case Study : IT DEL)</i>

The e-voting system uses blockchain technology is an electronic system for selecting and calculating votes using a distributed system for voting. At present the system that is still used for voting uses a centralized system that is center for collecting voting results. There are several problems that occur using e-voting systems such as on confidentiality and security of data voting. An attack that often occurs in the confidentiality of data voting is that there is a certain party or organization that has access rights to the central server on the system, so that someone can directly identify the identity of the voter who voted and each voting result of each voter. Whereas the attacks that occur on the security of data voting are the possibility of modifying the database voting, the result of voting becomes invalid or invalid.

In this final project the solution offered to overcome the problem in the e-voting system that is used today is to use a distributed system with a database that records all voting transactions shared with all parties participating or called the Blockchain Technology.

The purpose of building this e-voting system is to design and build an e-voting system using blockchain technology and prove the security of the results of voting data in aspects of accuracy, invulnerability, privacy, and verifiability achieved. To accelerate the development process of the e-voting system, one of the blockchain API is the SoChain API service. The SoChain API is a service that is used to connect to the e-voting system to create and retrieve voting transactions on the bitcoin address.

Testing for the e-voting system is done by making a test scenario on the functions contained in the system based on the use case scenario and to prove the aspects of the security method to be achieved narratively. The results of testing this system is the e-voting system using blockchain technology with security aspects including accuracy, invulnerability, privacy, and verifiability.

Keywords: *E-voting, Blockchain, Confidentiality, Security, API, Accuracy, Invulnerability, Privacy, Verifiability*

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS	ii
HALAMAN PENGESAHAN	iii
KATA PENGANTAR	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xii
DAFTAR LAMPIRAN.....	xiii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan.....	3
1.3 Lingkup	3
1.4 Pendekatan	4
1.5 Sistematika Penyajian	7
BAB 2 TINJAUAN PUSTAKA.....	9
2.1 Sistem <i>Electronic Voting</i>	9
2.2 Blockchain.....	10
2.2.1 Cara Kerja Blockchain	14
2.2.2 Metode Keamanan Sistem E-Voting Menggunakan Blockchain ...	16
2.2.3 Bitcoin.....	17
2.2.4 API (Application Programming Interface) Blockchain	19
2.3 Sistem Terdistribusi.....	19
2.4 Fungsi Hash.....	20
2.5 SHA (Secured Hash Algorithm)	21
2.6 Institut Teknologi Del	26
2.7 Web Application	27
2.8 Database	28
2.8.1 MySQL	28
2.8.2 Bahasa Pemograman yang Didukung	29
2.9 Related Works	30
2.10 Kesimpulan.....	44
BAB 3 ANALISIS	45
3.1 Pengenalan Proyek	45
3.2 Project Plan	45
3.3 Pengumpulan Data	45
3.3.1 Persiapan Survei.....	45
3.3.2 Pelaksanaan Survei	46
3.3.3 Hasil Survei.....	46
3.4 Analisis Sistem Polling	47
3.5 Analisis Rekam Polling.....	47
3.6 Current System	49
3.7 Target System System.....	53
3.7.1 User Characteristics	57
3.8 Analisis Environment.....	57

3.8.1	Operational Environment	58
3.9	Lingkungan Pengujian.....	58
3.9.1	Perangkat Lunak Pengujian	58
3.9.2	Perangkat Keras Pengujian	59
3.10	Analisis Teknologi Blockchain	59
3.11	Analisis Sistem E-Voting Menggunakan Teknologi Blockchain	64
3.12	Use Case Diagram	68
3.13	Use Case Scenario	69
BAB 4 DESIGN.....		75
4.1	Data Requirement.....	75
4.1.1	E-R Diagram	75
4.2	Desain Sistem E-Voting menggunakan Blockchain	76
4.2.1	Conceptual Data Model (CDM).....	76
4.2.2	Physical Data Model (PDM).....	76
4.2.3	Class Diagram	77
4.2.4	Sequence Diagram	78
4.2.5	Desain Antarmuka Sistem E-Voting menggunakan Blockchain	81
4.2.6	Functional Requirement	88
BAB 5 IMPLEMENTASI.....		90
5.1	Implementasi	90
5.1.1	Kebutuhan Implementasi.....	90
5.1.2	Tahapan Implementasi	91
5.2	Implementasi Aplikasi.....	92
BAB 6 PENGUJIAN.....		93
6.1	Prosedural Pengujian.....	93
6.2	Tujuan Pengujian.....	93
6.3	Persiapan Hardware dan Software untuk Pengujian	94
6.4	Scenario Pengujian	94
BAB 7 HASIL DAN PEMBAHASAN.....		108
7.1	Hasil	108
7.1.1	Tampilan Sistem E-Voting menggunakan Teknologi Blockchain	108
7.2	Pembahasan	121
7.3	Kendala.....	126
BAB 8 KESIMPULAN DAN SARAN.....		128
8.1	Kesimpulan.....	128
8.2	Saran	128
DAFTAR PUSTAKA.....		130
LAMPIRAN.....		xiv
Lampiran 1- Source Code Sistem		xiv
Lampiran 2 – Langkah Menginstal Sistem E-Voting menggunakan Blockchain		xxi

DAFTAR GAMBAR

Gambar 1.1 Metode Pendekatan Sistem	5
Gambar 2.1. Block Header [26]	11
Gambar 2.2. Ilustrasi blockchain[25].....	12
Gambar 2.3. Cara kerja sistem blockchain	15
Gambar 2.4. Metode generate dari public key ke bitcoin address [25]	18
Gambar 2.5. Fungsi Hash Satu Arah [19]	21
Gambar 2.6. Avalanche Effect [22]	23
Gambar 2.7. Tahap Processing pada SHA	24
Gambar 2.8. Tahap Hash Computation pada Hash	25
Gambar 2.9. Arsitektur Web Application [27]	28
Gambar 3.1. Current System Search Daftar Voting.....	49
Gambar 3.2. Current System Memasukkan polling	50
Gambar 3.3. Current System Mengedit Daftar polling	51
Gambar 3.4. Menghapus Daftar Polling	51
Gambar 3.5. Current System Download Rekapitulasi Polling.....	52
Gambar 3.6. Current System Melihat Detail Polling	53
Gambar 3.7. Login	54
Gambar 3.8. Target System Menambahkan Voting.....	54
Gambar 3.9. Target System Melihat Hasil Voting.....	55
Gambar 3.10. Melakukan Voting.....	55
Gambar 3.11. Membayar Bitcoin Address.....	56
Gambar 3.12. Proses Kerja transaksi dalam Teknologi Blockchain	59
Gambar 3.13. Struktur Block dalam Blockchain	61
Gambar 3.14. Rangkaian rantai block dalam blockchain	63
Gambar 3.15. Struktur penyimpanan transaksi voting di blockchain	64
Gambar 3.16. Struktur detail transaksi voting pada API SoChain	67
Gambar 3.17. Use Case Diagram.....	68
Gambar 4.1. E-R Diagram	75
Gambar 4.2. Conceptual Data Model	76
Gambar 4.3. Physical Data Model	77
Gambar 4.4. Class Diagram	77
Gambar 4.5. Sequence Diagram Login	78
Gambar 4.6. Sequence Diagram Membuat Daftar Voting	79
Gambar 4.7. Sequence Diagram Melakukan Vote	79
Gambar 4.8. Sequence Diagram Membayar Bitcoin Address	80
Gambar 4.9. Sequence Diagram Melihat Hasil Voting	80
Gambar 4.10. Desain Sistem – Login Administrator.....	81
Gambar 4.11. Desain Sistem – Beranda	81
Gambar 4.12. Desain Sistem – Daftar Bitcoin Address.....	82
Gambar 4.13. Desain Sistem – Membuat Daftar Kandidat.....	82
Gambar 4.14. Desain Sistem – Daftar Kandidat.....	83
Gambar 4.15. Desain Sistem – Membuat Daftar Voting	84
Gambar 4.16. Desain Sistem – Daftar Voting	85
Gambar 4.17. Desain Sistem – Rincian Daftar Voting	85
Gambar 4.18. Desain Sistem – Halaman Token	86

Gambar 4.19. Desain Sistem – Halaman Melakukan Vote.....	86
Gambar 4.20. Desain Sistem – Hasil Voting	87
Gambar 4.21. Desain Sistem – Daftar Voting untuk Voter	87
Gambar 4.22. Desain Sistem – Halaman Voting Selesai	88
Gambar 7.1. Tampilan Login untuk Administrator	108
Gambar 7.2. Tampilan Beranda	109
Gambar 7.3. Tampilan Menambah Voting	110
Gambar 7.4. Tampilan Daftar Voting	111
Gambar 7.5. Tampilan Rincian Daftar Voting.....	112
Gambar 7.6. Tampilan Membuat Daftar Kandidat	113
Gambar 7.7. Tampilan Daftar Kandidat	114
Gambar 7.8. Tampilan Daftar Bitcoin Address	115
Gambar 7.9. Tampilan Daftar Voting untuk Voter	116
Gambar 7.10. Tampilan Email untuk Voting.....	116
Gambar 7.11. Tampilan Form Memasukkan Token	117
Gambar 7.12. Tampilan Daftar Voting untuk Melakukan Vote	118
Gambar 7.13. Tampilan Hasil Voting	119
Gambar 7.14. Tampilan Halaman Voting Selesai.....	120
Gambar 7.15. Tampilan Detail Transaksi Voting pada Blockchain	120
Gambar 7.16. Arsitektur Sistem E-Voting menggunakan Teknologi Blockchain	122

DAFTAR TABEL

Tabel 2.1. Related Works.....	30
Tabel 3.1. Use Case Scenario Login	69
Tabel 3.2. Use Case Scenario Membuat Voting	69
Tabel 3.3. Use Case Scenario Menambahkan Kandidat	70
Tabel 3.4. Use Case Scenario MenambahkanVoter.....	71
Tabel 3.5. Use Case Scenario Membayar Bitcoin Address	71
Tabel 3.6. Use Case Scenario Melakukan Vote	72
Tabel 3.7. Use Case Scenario Melihat Hasil Voting.....	74
Tabel 4.1. Functional Requirement.....	88
Tabel 5.1. Spesifikasi Hardware dan Software	90
Tabel 6.1. Pengujian Aunthentication.....	94
Tabel 6.2. Pengujian Membuat Daftar Voting.....	95
Tabel 6.3. Pengujian Melakukan Vote	98
Tabel 6.4. Pengujian Melihat Hasil Voting	104
Tabel 6.5. Pengujian Membayar Bitcoin Address	105

DAFTAR LAMPIRAN

Lampiran 1. Source Code Fungsi untuk mengirim email ke voter	xiv
Lampiran 2. Source Code Fungsi untuk mengenerate Token dan BitcoinAddress untuk Voter	xv
Lampiran 3. Source Code Fungsi untuk melakukan pembayaran ke voter agar voter dapat melakukan voting	xvi
Lampiran 4. Source Code Fungsi untuk melakukan pemilihan (Voter melakukan Voting)	xviii
Lampiran 5. Source Code Fungsi hex2bin untuk mengonversi OP_Return (hexadecimal) menjadi biner (character)	xviii
Lampiran 6. Source code untuk proses penghitungan suara	xx
Lampiran 7. Cara Menginstal Sistem E-Voting menggunakan Teknologi Blockchain	xxi

BAB 1

PENDAHULUAN

Pada bab pendahuluan dijelaskan mengenai latar belakang pemilihan topik, tujuan penggerjaan Tugas Akhir, lingkup kajian pada Tugas Akhir, pendekatan yang dilakukan untuk penggerjaan Tugas Akhir, dan sistematika penyajian yang dilakukan dalam penggerjaan Tugas Akhir.

1.1 Latar Belakang

Seiring dengan berkembangnya teknologi informasi, sistem pemilihan umum di Indonesia telah beralih menggunakan bantuan teknologi informasi untuk menyelenggarakan proses pemilihan menjadi elektronik. Pemilihan yang dilakukan dengan menggunakan teknologi informasi disebut dengan elektronik voting (e-voting). Pada sistem e-voting penggunaan kertas sudah diminimalkan karena sistem ini sudah berbasis teknologi digital. Saat ini sistem e-voting sudah digunakan di sektor perguruan tinggi sebagai sarana mengambil keputusan tertentu yang bersifat umum, contohnya pada kegiatan mahasiswa di kampus. Beberapa perguruan tinggi di Indonesia seperti IT DEL, ITB, IPB, UNESA, dan perguruan tinggi lainnya telah menggunakan sistem e-voting untuk kegiatan pemilihan mahasiswa di kampus seperti pemilihan mahasiswa teladan, pemilihan ketua BEM, pemilihan ketua organisasi, pemilihan ketua prodi, dan lain sebagainya [5].

Skema e-voting adalah satu set *protocol* yang menjaga keamanan atau kerahasiaan pemilih dalam melakukan pemilihan dan perhitungan suara. Tujuan dari keamanan sistem e-voting adalah menjamin privasi atau kerahasiaan pemilih dan keakuratan pilihan. Keamanan sistem e-voting memiliki beberapa kriteria yang mencakup *accuracy*, *invulnerability*, *privacy*, dan *verifiability*.

Dengan dibuatnya sistem e-voting ini memungkinkan proses pemilihan yang diselenggarakan semakin mudah, mempersingkat waktu pelaksanaan, dan meminimalisir biaya anggaran yang diperlukan untuk e-voting. Namun sistem e-voting yang digunakan saat ini masih menimbulkan beberapa permasalahan pada prinsip dasar pemilu yaitu kerahasiaan data dan keamanan hasil voting [1].

Sistem e-voting yang ada masih menggunakan model jaringan terpusat dengan bantuan pihak ketiga yakni sebuah server menjadi pusat dari pengumpulan hasil

voting. Contohnya serangan pada kerahasiaan data pada sistem e-voting adalah jika ada pihak ketiga yang berhasil mengakses server tersebut, maka identitas pemilih dan data yang dipilihnya akan mudah diketahui secara langsung sehingga menimbulkan salah satu prinsip pemilu atas kerahasiaan tidak terjadi. Sedangkan contoh serangan keamanan informasi adalah melakukan manipulasi atau mengubah hasil voting. Jika ada orang dalam yang memiliki hak akses masuk server dan memiliki wewenang untuk mengubah data, maka data hasil perolehan voting tersebut menjadi tidak sah karena hasil suara yang telah dihitung tidak terkoreksi dengan benar. Keberhasilan penyerangan terhadap kerahasiaan dan keamanan data voting dapat menyebabkan risiko yang besar untuk merusak e-voting. Untuk mengatasi hal tersebut dibutuhkan teknologi untuk mengurangi permasalahan pemungutan suara. Salah satu teknologi yang sedang berkembang untuk mengatasi risiko tersebut adalah menggunakan teknologi blockchain.

Blockchain pada dasarnya adalah basis data terdistribusi dari catatan atau buku besar umum dari semua transaksi yang telah dilaksanakan dan dibagikan di antara para pihak yang berpartisipasi [2]. Teknologi blockchain secara umum bersifat *peer-to-peer*, dalam arti sebuah data dapat berupa pesan, uang, atau informasi penting dapat dipindahkan dari satu pengguna ke pengguna yang lain tanpa bantuan pihak ketiga [3]. Jaringan blockchain juga bersifat transparan, terdistribusi, dan berbasis konsensus. Melakukan transaksi berbasis blockchain tidak berarti bahwa setiap orang dapat melihat bagaimana setiap orang melakukan transaksi. Namun hasil transaksi yang terenkripsi tidak hanya masuk ke satu server, tetapi seluruh jaringan blockchain yang terdistribusi dan semua transaksi di jaringan tersebut sepenuhnya transparan. Transaksi dienkripsi dan divalidasi pada jaringan blockchain oleh mekanisme konsensus dan setiap transaksi didaftarkan secara *public* pada salinan buku besar yang didistribusikan. Ini berarti siapapun dapat membaca, mengunduh, menyimpan, dan menghitung transaksi blockchain transaksi tetapi tidak ada yang tahu siapa yang memberikan transaksi tersebut [4].

Pada pengerjaan tugas akhir ini akan dilakukan "Pembangunan Sistem E-voting Menggunakan Teknologi Blockchain Studi Kasus Institut Teknologi Del" untuk

mengatasi permasalahan-permasalahan server terpusat yang dapat diretas oleh pihak ketiga, kerahasiaan data voting, dan keamanan hasil voting.

Oleh karena itu, peneliti akan membangun sistem e-voting menggunakan teknologi blockchain berbasis web dimana sistem e-voting ini akan terhubung dengan blockchain. Setelah pengguna selesai melakukan voting sistem akan mengirimkan transaksi voting ke jaringan blockchain. Teknologi blockchain bersifat transparan yaitu semua transaksi voting yang telah terdaftar dibroadcast pada jaringan blockchain. Setiap voter yang telah terdaftar pada sistem dapat membaca, mengunduh, dan menghitung transaksi voting di blockchain, tetapi tidak ada satupun yang mengetahui hasil suara masing-masing voter dan identitas voter yang memilih kandidat tersebut.

Dengan dibangunnya sistem e-voting menggunakan teknologi blockchain diharapkan dapat mengatasi serangan atau permasalahan yang terjadi pada keamanan dan kerahasiaan data voting pada sistem.

1.2 Tujuan

Tujuan dari pengerjaan Tugas Akhir ini yaitu :

1. Merancang dan membangun sistem e-voting dengan menggunakan teknologi blockchain .
2. Membuktikan keamanan hasil data voting dalam aspek *accuracy*, *invulnerability*, *privacy*, dan *verifiability* tercapai.

1.3 Lingkup

Lingkup masalah yang ingin dicakup dalam penelitian adalah :

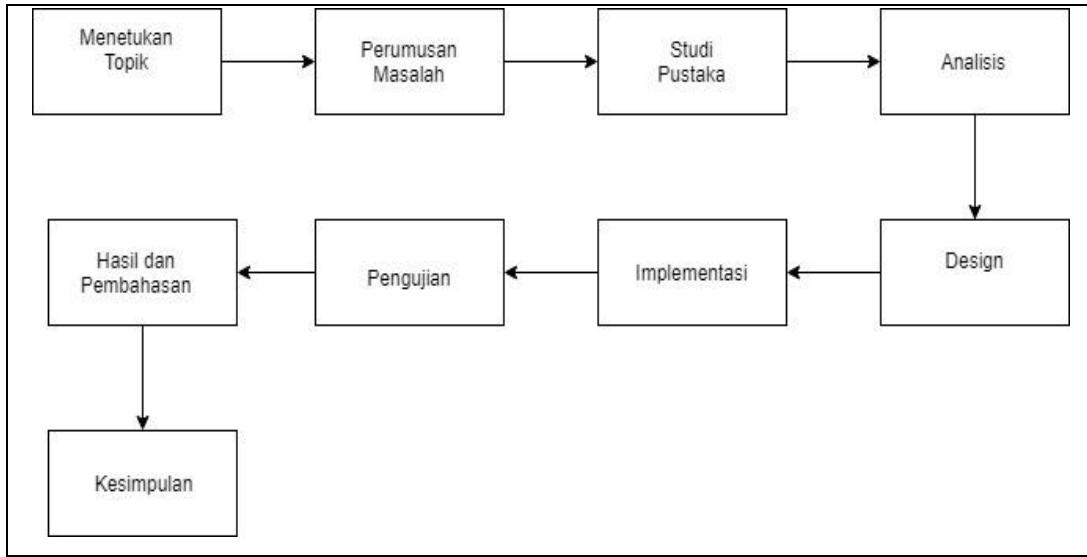
1. Teknologi yang digunakan untuk merancang dan membangun sistem hasil e-voting dengan menggunakan teknologi Blockchain.
2. Pembangunan sistem e-voting menggunakan teknologi blockchain terdiri dari satu jenis *user interface* yaitu versi web.
3. Pembangunan sistem e-voting menggunakan teknologi blockchain mencakup kegiatan pemilihan di Institut Teknologi Del seperti Pemilihan ketua BEM, Mahasiswa Teladan, panitia PCA, dan panitia Epiphania.

4. Pembangunan sistem e-voting akan diimplementasikan menggunakan framework Yii2, bahasa pemrograman PHP dan Javascript, Library Bitcoin PHP, dan BitcoinJS.
5. Salah satu layanan API Blockchain yang digunakan untuk mempercepat proses development sistem e-voting adalah API SoChain.
6. Untuk menjalankan sistem ini diperlukan koneksi internet yang stabil.

1.4 Pendekatan

Metode penelitian yang akan digunakan dalam pelaksanaan Tugas Akhir ini adalah metode penelitian kuantitatif. Penelitian kuantitatif merupakan penelitian yang menekankan pada data numerikal (angka) yang diolah dengan metode statisika. Menurut Subana dan Sudrajat penelitian kuantitatif dipakai untuk menguji suatu teori, menyajikan suatu fakta, dan untuk menunjukkan hubungan antar variabel dan adapula yang sifatnya mengembangkan konsep dan mengembangkan pemahaman. Sumber data yang akan digunakan untuk mendukung pengerjaan Tugas Akhir adalah data sekunder. Data sekunder adalah data yang diperoleh dari sumber yang sudah ada. Contoh data sekunder adalah sumber tertulis seperti sumber buku, paper, majalah ilmiah, jurnal karya ilmiah, dan sumber-sumber bacaan lainnya seperti internet lainnya yang dapat dijadikan sebagai acuan pembahasan masalah dalam penelitian yang akan dilakukan.

Metode pengembangan sistem yang digunakan penulis dalam pengerjaan Tugas Akhir ini dapat dilihat pada Gambar 1.1 yang dimulai dengan tahapan menentukan topik, perumusan masalah, studi pustaka, desain, analisis, implementasi, pengujian, hasil dan pembahasan, dan kesimpulan.



Gambar 1.1 Metode Pendekatan Sistem

Keterangan :

1. Menentukan Topik

Tahap ini adalah tahap pertama dalam penggerjaan Tugas Akhir. Pada tahap ini dilakukan pembahasan dan penentuan topik dengan tujuan untuk mengetahui mengapa topik ini harus dibuat.

2. Perumusan Masalah

Pada tahap ini penulis mengumpulkan data atau mencari referensi terkait topik untuk mencari judul yang spesifik dari berbagai jurnal. Pada tahapan ini peneliti akan mengklasifikasikan masalah dan solusi yang mungkin dilakukan untuk mendefinisikan sistem apa yang akan dibangun.

3. Studi Pustaka

Pada tahap ini penulis akan mencari informasi untuk memperluas pemahaman mengenai topik dengan mengumpulkan dokumen-dokumen sebagai referensi seperti buku, jurnal, artikel, paper, makalah, maupun situs dari internet. Pada tahap ini peneliti akan membuat kesimpulan bagaimana sistem akan yang akan dibangun melalui informasi yang telah dikaji penulis. Penulis juga akan membandingkan terhadap metode yang telah dipakai sebelumnya yaitu algoritma, tools, yang dipakai, tahap penggerjaan, dan kesimpulan dari penelitian.

4. Analisis

Pada tahap ini peneliti akan memahami dan menganalisis bagaimana cara kerja dari setiap metode yang akan digunakan untuk teknologi blockchain dan pembangunan sistem e-voting menggunakan teknologi blockchain. Pada tahap analisis menjawab pertanyaan siapa yang akan menggunakan sistem, fungsi yang akan dilakukan sistem, dan kapan akan digunakan. Selama tahap ini, tim peneliti akan mengidentifikasi sistem apa yang berjalan saat ini, pengembangan sebuah konsep pada sistem yang akan dibangun.

5. Desain

Pada tahap ini peneliti akan melakukan perancangan bagaimana sistem akan beroperasi baik dalam hal perangkat keras, perangkat lunak, design aplikasi seperti aplikasi yang dibangun yaitu *domain model*, CDM, PDM, *class diagram*, dan *sequence diagram*, serta design interface dari sistem yang akan dibangun.

Peneliti juga akan melakukan perbandingan terhadap rancangan interface dari hasil penelitian sebelumnya sehingga penulis dapat menetapkan *design interface* yang akan dibuat.

6. Implementasi

Pada tahap ini design yang telah ditetapkan kemudian diimplementasikan menjadi sebuah sistem yang dapat berjalan sesuai dengan kebutuhan. Dalam tahap ini metode yang telah ditetapkan sebelumnya diimplementasikan menggunakan bahasa pemrograman yang telah ditentukan pada sistem berdasarkan tahap *design*.

7. Pengujian

Pada tahap ini hasil implementasi mendapatkan pengujian. Hal ini dilakukan untuk memastikan dan menjamin bahwa sistem telah berjalan sesuai dengan implementasi yang dilakukan dan tidak memiliki *error*.

8. Hasil dan Pembahasan

Pada tahap ini berisi informasi mengenai hasil yang diperoleh di akhir pelaksanaan Tugas Akhir. Hasil dapat berupa produk, rancangan sistem, hasil analisis terhadap studi perbandingan, dan lain-lain. Hasil yang

diperoleh dituliskan analisis yang lebih mendalam terhadap hasil yang diperoleh. Selain menyajikan hasil–hasil kajian pada tahap ini juga disampaikan uraian penjelasan singkat atas hasil tersebut.

9. Kesimpulan

Pada tahap ini dilakukan pengambilan sebuah kesimpulan mengenai penggerjaan Tugas Akhir. Kesimpulan yang diharapkan sesuai dengan hasil implementasi yang telah dilakukan sebelumnya dan dapat memenuhi kebutuhan sistem yang telah dibangun .

1.5 Sistematika Penyajian

Dokumen Laporan Tugas Akhir ini terdiri dari delapan bab.

1. Bab I Pendahuluan

Pada Bab ini dijelaskan tentang latar belakang, tujuan, lingkup, pendekatan, dan sistematika penyajian.

2. Bab II Tinjauan Pustaka

Pada Bab ini dijelaskan tentang tinjauan pustaka yang membahas dasar-dasar teori yang relevan dengan topik tugas akhir.

3. Bab III Analisis

Pada Bab ini dijelaskan tentang analisis mengenai pengenalan proyek, perencanaan proyek, analisis yang dilakukan terhadap *current system*, dan rancangan sistem yang akan dikembangkan (*target system*).

4. Bab IV Desain

Pada Bab ini dijelaskan tentang perancangan dari sistem yang akan dikembangkan dalam bentuk *data requirement*, *conceptual data*, *physical data*, *class diagram*, dan *sequence diagram*.

5. Bab V Implementasi

Pada Bab ini merupakan implementasi yang menjelaskan deskripsi umum sistem yang meliputi kebutuhan implementasi, batasan implementasi, dan implementasi aplikasi. Pada bab ini juga dijelaskan mengenai langkah-langkah awal implementasi dari mulai persiapan perangkat keras dan perangkat lunak yang diperlukan.

6. Bab VI Pengujian

Pada bab ini dijelaskan mengenai scenario pengujian yang akan dilakukan terhadap sistem yang akan dibangun.

7. Bab VII Hasil dan Pembahasan

Pada bab ini dijelaskan mengenai hasil yang didapat setelah melakukan tahap implementasi sistem, kendala yang dihadapi dalam pembangunan sistem, dan kekurangan pada sistem setelah diimplementasi.

8. Bab VIII Kesimpulan dan Saran

Pada bab ini dijelaskan mengenai kesimpulan dari produk yang anda hasilkan, proses pengerjaan, pelaksanaan Tugas Akhir, maupun kesimpulan tentang kesan yang diperoleh selama pelaksanaan Tugas Akhir serta memberikan saran apabila memungkinkan sistem ini untuk dilanjutkan atau dikembangkan lagi.

BAB 2

TINJAUAN PUSTAKA

Pada bab Tinjauan Pustaka dijelaskan informasi teoritis dan pustaka yang mendukung untuk dapat digunakan dalam penggerjaan Tugas Akhir.

2.1 Sistem *Electronic Voting*

E-voting berasal dari kata *electronic voting* yang mengacu pada penggunaan teknologi informasi pada pelaksanaan pemungutan suara. E-voting adalah suatu metode pemungutan suara dan perhitungan suara dalam pemilihan dengan menggunakan perangkat elektronik [1]. Dengan kata lain e-voting merupakan pemungutan suara yang proses pelaksanaannya mulai dari pendaftaran pemilih, pelaksanaan pemilihan, perhitungan suara dan pengiriman hasil suara secara elektronik (digital) [5]. Pilihan teknologi yang digunakan dalam implementasi dari e-voting bermacam-macam, seperti penggunaan *smart card* untuk otentikasi pemilih, penggunaan internet sebagai sistem pemungutan suara, penggunaan *touch screen* sebagai pengganti kartu suara, dan masih banyak variasi teknologi yang digunakan [6].

E-voting bertujuan meningkatkan partisipasi, menurunkan biaya pemilu, dan meningkatkan akurasi hasil pemilu. Dengan e-voting perhitungan suara akan lebih cepat, bisa menghemat biaya pencetakan surat suara, pemungutan suara lebih sederhana, dan peralatan e-voting dapat digunakan berulang kali [6].

Namun sistem e-voting memiliki beberapa kelemahan yaitu terbatasnya keterbukaan, berpotensi melanggar kerahasiaan pemilihan, khususnya dalam sistem yang melakukan autentikasi pemilih dan kandidat yang dipilih, risiko manipulasi oleh orang yang mempunyai hak akses ke sistem, meningkatnya biaya pembelian sistem dan pemeliharaan sistem e-voting, dan meningkatnya persyaratan keamanan untuk melindungi sistem voting selama pemilu dan pemilu yang akan dilakukan selanjutnya termasuk selama pengangkutan, penyimpanan, dan pemeliharaan.

Menurut International IDEA (2011), pelaksanaan evoting secara umum dikategorikan ke dalam empat tipe sebagai berikut [8] :

1. Mesin pemungutan suara dengan menggunakan pencatatan langsung elektronik (DRE).

2. Sistem OMR yang didasarkan pada mesin pemindai yang dapat mengenali pilihan pemilih di surat suara.
3. Mesin pencetak surat suara (EBP) menghasilkan kertas yang dapat dibaca mesin atau koin elektronik yang berisikan pilihan pemilih.
4. Sistem pemilihan melalui Internet yaitu saat suara diberikan melalui Internet ke server pusat penghitungan.

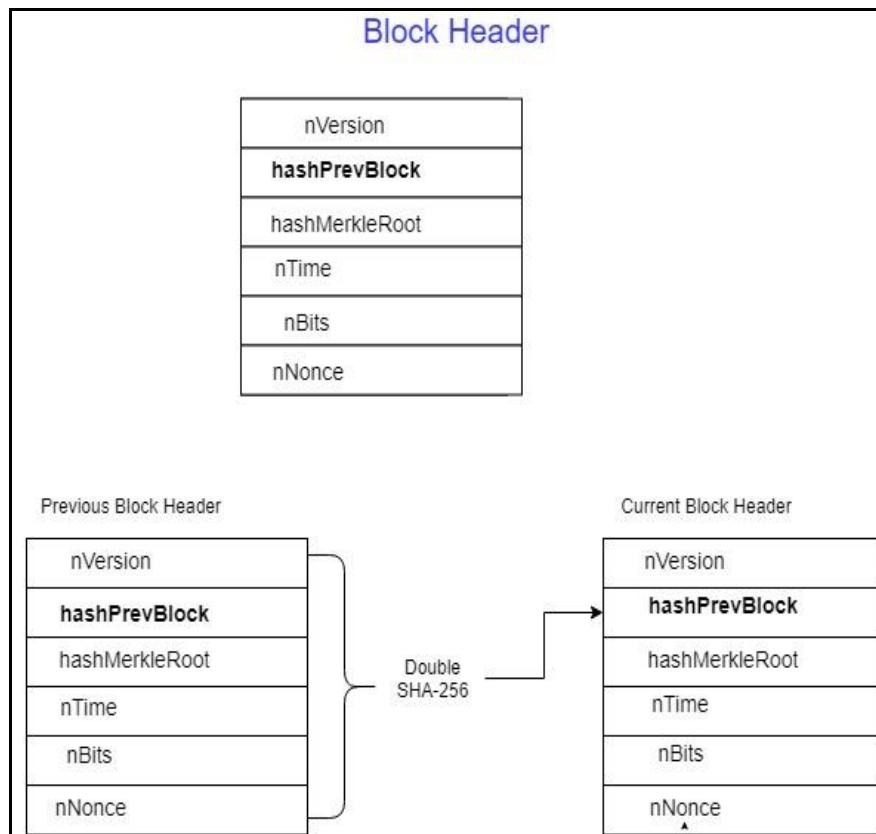
Menurut peneliti sistem e-voting merupakan sistem elektronik yang terkomputerisasi untuk menggantikan sistem konvensional dengan mengadopsi model server terpusat (sentralisasi) untuk melakukan pemungutan suara dalam rangka mempercepat proses pemilihan, menghasilkan perhitungan suara lebih akurat, menghemat biaya kertas suara, alat e-voting dapat digunakan berulang kali, dan menyediakan akses bagi pemilih yang memiliki keterbatasan fisik, dan waktu untuk mendatangi tempat pemungutan suara (TPS).

2.2 Blockchain

Blockchain pada dasarnya adalah basis data terdistribusi dari catatan atau buku besar umum dari semua transaksi atau peristiwa digital yang telah dilaksanakan dan dibagikan di antara para pihak yang berpartisipasi [9]. Blockchain pertama kali muncul pada tahun 2008 oleh Satoshi Nakamoto. Bitcoin adalah salah satu bentuk mata uang digital (digital currency) yang memanfaatkan teknologi blockchain pertama kalinya. Blockchain membawa konsep fundamental yang mengubah sifat ledger yang semula terpusat (*centralised ledger*) menjadi terdistribusi (*decentralised ledger*). Ledger tidak dipegang oleh satu pihak atau dua pihak, melainkan direplikasi dan didistribusikan kepada semua pihak yang berada dalam sistem. Transaksi menggunakan teknologi Blockchain bersifat *peer-to-peer*, dalam arti sebuah data dapat berupa pesan, uang, atau informasi penting dapat dipindahkan dari satu pengguna ke pengguna yang lain tanpa bantuan pihak ketiga untuk memprosesnya. Dengan Blockchain, tidak lagi perlu lagi bergantung pada satu server karena seluruh transaksi tereplikasi ke seluruh jaringan sehingga terhindar dari berbagai bentuk penipuan seperti data yang dimodifikasi, *server down*, atau akun yang diretas [10].

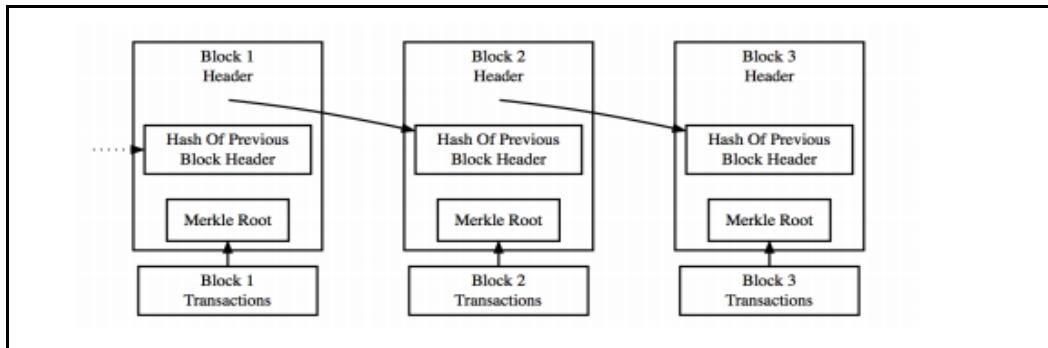
Sebuah blockchain menyimpan transaksi dalam sebuah blok sampai transaksi selesai dilakukan. Satu blok berisi banyak record transaksi. Blok-blok ini

tersusun secara linear berdasarkan urutan waktu masing-masing, blok awal dalam blockchain dikenal sebagai “blok kejadian”. Blok awal biasanya *hardcoded* ke dalam perangkat lunak. Blok tersebut khusus karena tidak berkaitan dengan blok sebelumnya atau disebut dengan blok genesis. Setelah blok genesis telah diinisialisasi “blok satu” dibuat dan ketika lengkap dilampirkan ke blok genesis. Setelah blok memiliki bagian data transaksi, salinan setiap transaksi tersebut di hash, dan kemudian hash dipasangkan dan dihash lagi, ini terus berlanjut sampai satu hash tetap yang dikenal sebagai akar *merkle*. Fungsi hash pada blok digunakan untuk mengambil salinan data transaksi dari blok sebelumnya untuk blok yang akan diciptakan. Blok header adalah tempat akar merkle disimpan. Blok header memiliki enam parameter yaitu *version*, *hash value of the previous root*, *hash value of the Merkle root*, *Timestamps*, *number of bits*, dan *nonces*. Blok dihubungkan oleh item *hashPrevBlock* dengan blok lainnya. Tampilan detail dari header blok dengan cakupan didalamnya digambarkan pada Gambar 2.1 dimana *hashPrevBlock* adalah nilai hash double SHA-256. Sehingga semua blok terkait satu sama lain dan semua history transaksi dicatat di blockchain [26].



Gambar 2.1. Block Header [26]

Untuk memastikan bahwa transaksi tidak dapat dimodifikasi setiap blok juga menyimpan catatan dari header blok sebelumnya, ini berarti untuk mengubah data Anda harus memodifikasi blok yang mencatat transaksi serta semua blok berikut. Seperti terlihat pada Gambar 2.2 ilustrasi blockchain berikut.



Gambar 2.2. Ilustrasi blockchain[25]

Blockchain menunjukkan berapa waktu yang dibutuhkan untuk sebuah untuk sebuah block ditambahkan. Block berisi transaksi yang terjadi pada waktu tertentu. Nilai hash dari block sebelumnya dan block yang saat ini akan menjadi input dari nilai hash untuk block selanjutnya. Setiap nilai hash dari sebuah block dihitung dari nilai hash block sebelumnya, dan transaksi dicatat di blok. Karena hash dari block sebelumnya digunakan untuk menghasilkan nilai dari hash blok berikutnya, block berikutnya akan dirantai dengan block sebelumnya, memperkuat integritas semua block sebelumnya. Setiap block anterior berisi informasi tentang hash dari block sebelumnya seperti yang ditunjukkan pada Gambar 3. Setiap block saling berhubungan dengan blok berikutnya. Jika ada data dalam block yang dimodifikasi, nilai hash dari block akan diubah. Hasilnya adalah bahwa hash dari semua block yang terbaru akan diubah. Rantai block yang seperti ini tidak akan diterima sebagai rantai block yang valid dan akan ditolak [25].

Sebuah blockchain dirancang untuk diakses di seluruh jaringan peer to peer, setiap node berkomunikasi dengan node lain untuk pertukaran blok dan transaksi. Setelah terhubung ke jaringan, setiap mulai mengirim pesan ke node lain di jaringan yang akan menciptakan metode peer to peer dan terdesentralisasi. Tujuan dari node dalam jaringan adalah untuk memvalidasi transaksi yang belum dikonfirmasi dan blok yang baru ditambah. Sebelum node baru mulai melakukan

ini terlebih dahulu melakukan pengunduhan blok awal. Unduhan blok awal membuat unduhan blok baru dan memvalidasi semua blok dari blok satu ke blockchain terbaru, setelah ini dilakukan, node dianggap disinkronkan [8].

Blockchain sebagai buku besar digital memiliki tiga property kunci yaitu :

1. Sistem ini bersifat terbuka siapapun dapat menggunakannya, mendistribusikan, dan membangun kode sumber blockchain.
2. Salinan data hasil transaksi didistribusikan, hasil data transaksi tidak hanya terdaftar dan diproses di server terpusat.
3. Sistem blockchain bersifat transparan. Semua hasil voting yang sudah dihitung dalam jaringan blockchain dapat dipantau oleh semua node yang terlibat.

Pada umumnya teknologi blockchain digunakan untuk mengakses, memverifikasi, dan mentransmisikan data jaringan melalui node terdistribusi. Teknologi blockchain menggunakan jaringan peer to peer untuk mencapai operasi data yang terdesentralisasi.

Teknologi Blockchain memiliki karakteristik utama sebagai berikut :

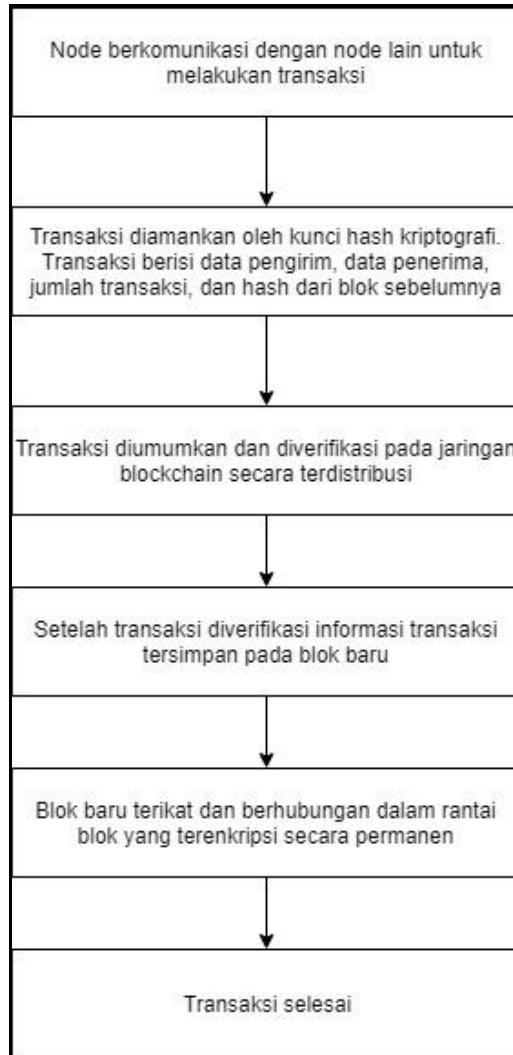
1. Kunci publik infranstruktur digunakan untuk mengidentifikasi identitas pemilih dan menjaga keamanan. Setiap akun pemilih di blockchain memiliki public key dan private key yang digunakan untuk mengirim dan menerima transaksi. Setelah private key mengenkripsi data transaksi, penerima kemudian menggunakan public key untuk mendekripsi pesan dan identitas pengirim dapat dikonfirmasikan.
2. Teknik peer to peer digunakan untuk pengiriman dan pendistribusian pesan, memungkinkan setiap node terhubung satu sama lain untuk saling bertukar pesan. Transaksi disimpan dalam buku besar dimana setiap node dalam blockchain dapat memverifikasi transaksi pada struktur akses yang terdesentralisasi.
3. Penyimpanan dan penautan data untuk menghasilkan nilai hash dan blok tersebut berkaitan dengan blok sebelumnya dengan nilai-nilai hash untuk membangun blockchain. Blok tersebut merinci catatan blok seperti *time-stamp*, kuantitas transaksi, nilai hash, dan lain-lain.

2.2.1 Cara Kerja Blockchain

Blockchain pada sistem transaksi terdiri dari dua jenis record data yang akan disimpan yaitu hasil transaksi dan blok. Setiap blok pada blockchain berisi fungsi hash kriptografi yang berfungsi untuk mengambil data dari blok sebelumnya dan mengubahnya menjadi string dalam bentuk karakter. Hash memungkinkan setiap node memverifikasi transaksi di dalam jaringan terdistribusi. Transaksi yang sudah diverifikasi dimasukkan dalam blok-blok yang sudah dirantai secara permanen dengan blok hasil transaksi sebelumnya dan sesudah diverifikasi. Teknologi blockchain bersifat terdentralisasi, setiap komputer dalam jaringan blockchain memiliki salinan semua data transaksi yang terus diperbarui dengan blok baru. Tidak ada server terpusat yang memegang salinan transaksi karena setiap blok dalam jaringan blockchain harus diperbarui ke setiap server yang terlibat dalam jaringan blockchain secara terdistribusi. Setiap komponen dalam jaringan ini terhubung satu sama lain untuk penyampaian hasil transaksi ke semua komponen. Komponen yang dimaksud terdiri dari kumpulan node yang saling terhubung dalam jaringan terdistribusi. Node tersebut saling bekomunikasi untuk pengiriman transaksi ke semua node yang terhubung.

Dengan sistem pencatatan transaksi yang terdistribusi dan terikat dengan rantai blok yang terenkripsi membuat platform ini sangat aman. Beberapa hambatan yang ada pada blok transaksi yang terenkripsi. Hambatan pertama yaitu untuk dapat meretas satu transaksi pada server berarti harus juga dapat meretas blok data transaksi sebelum dan sesudahnya. Kedua, dengan sistem yang terdistribusi pada banyak komputer yang digunakan sebagai salinan data transaksi, untuk dapat meretas satu salinan blockchain seorang peretas harus mendapatkan verifikasi dari server penyedia salinan data transaksi lainnya. Oleh karena itu teknologi blockchain ini memberikan tingkat keamanan yang tinggi.

Berikut Gambar 2.3 cara kerja sistem blockchain.



Gambar 2.3. Cara kerja sistem blockchain

Keterangan cara kerja sistem blockchain :

Dalam transaksi blockchain pengguna melakukan transaksi dengan pengguna lainnya. Setelah melakukan transaksi, transaksi akan diamankan menggunakan kunci hash kriptografi. Data transaksi berisi data pengirim, data penerima, dan jumlah transaksi. Fungsi hash kriptografi pada blok berfungsi untuk mengambil data dari blok sebelumnya dan mengubahnya menjadi string (karakter). Sebelum node baru dibuat dilakukan terlebih dahulu dilakukan pengunduhan blok awal. Selanjutnya hasil transaksi tersebut akan diumumkan dan diverifikasi pada jaringan blockchain secara terdistribusi, apabila transaksi tersebut valid maka akan tercipta unduhan blok baru dimana hasil transaksi tersebut dicatat dan disimpan dalam blok baru. Blok tersebut tersusun secara beraturan dan berkaitan dengan blok sebelumnya. Blok baru yang telah tercipta terikat satu sama lain dan

berhubungan dalam satu rangkaian rantai blok yang terenkripsi secara permanen. Setelah itu transaksi dianggap selesai.

2.2.2 Metode Keamanan Sistem E-Voting Menggunakan Blockchain

Menurut Howard Raharjo keamanan informasi merupakan suatu usaha pencegahan atas serangan untuk mendapatkan sesuatu dari sistem informasi, baik melalui akses yang tidak semestinya maupun penggunaan yang tidak semestinya [12]. Begitu juga untuk aspek keamanan yang harus dipenuhi dalam pengembangan sistem e-voting dengan tujuan untuk memberikan keamanan penyelenggaraan pemilihan e-voting pada dasar pemilu di Indonesia yaitu langsung, umum, bebas, rahasia, jujur, dan adil.

Cranor dan Cytron menyatakan bahwa e-voting harus memiliki parameter yang bisa dijadikan sebagai pedoman. Pernyataan tersebut dikenal dengan istilah *Golden Rules e-voting* yang mencakup sebagai berikut [13]:

1. Accuracy

Suatu sistem akurat jika tidak mungkin hasil suara dapat dimodifikasi, tidak mungkin hasil vote yang divalidasi dihilangkan dari perhitungan akhir, dan tidak mungkin suara yang tidak sah untuk dihitung dalam perhitungan akhir.

Dalam sistem yang paling akurat penghitungan suara akhir harus sempurna, informasi bebas dari kesalahan, baik karena tidak ada ketidakakuratan dapat diperkenalkan atau karena semua ketidakakuratan diperkenalkan dapat dideteksi dan diperbaiki. Sistem yang akurat dapat mendeteksi tetapi belum tentu benar ketidakakuratannya.

2. Invulnerability

Sebuah sistem e-voting disebut sebagai *invulnerability* jika hanya mengizinkan pemilih yang berhak untuk memilih dan memastikan bahwa masing-masing pemilih yang telah memenuhi syarat dapat memilih hanya sekali.

3. Privacy

Suatu sistem e-voting bersifat *privacy* jika tidak ada otoritas pemilihan atau orang lain dapat menghubungkan surat suara apa pun dengan pemilih

yang memberikannya, dan tidak ada pemilih yang dapat membuktikan bahwa ia memilih dengan cara tertentu serta tidak ada pemilih yang mengetahui hasil suara dari orang lain.

4. Verifiability

Suatu hasil voting dapat diverifikasi jika ada yang secara independen dapat memverifikasi bahwa semua suara yang telah dihitung terkoreksi dengan benar.

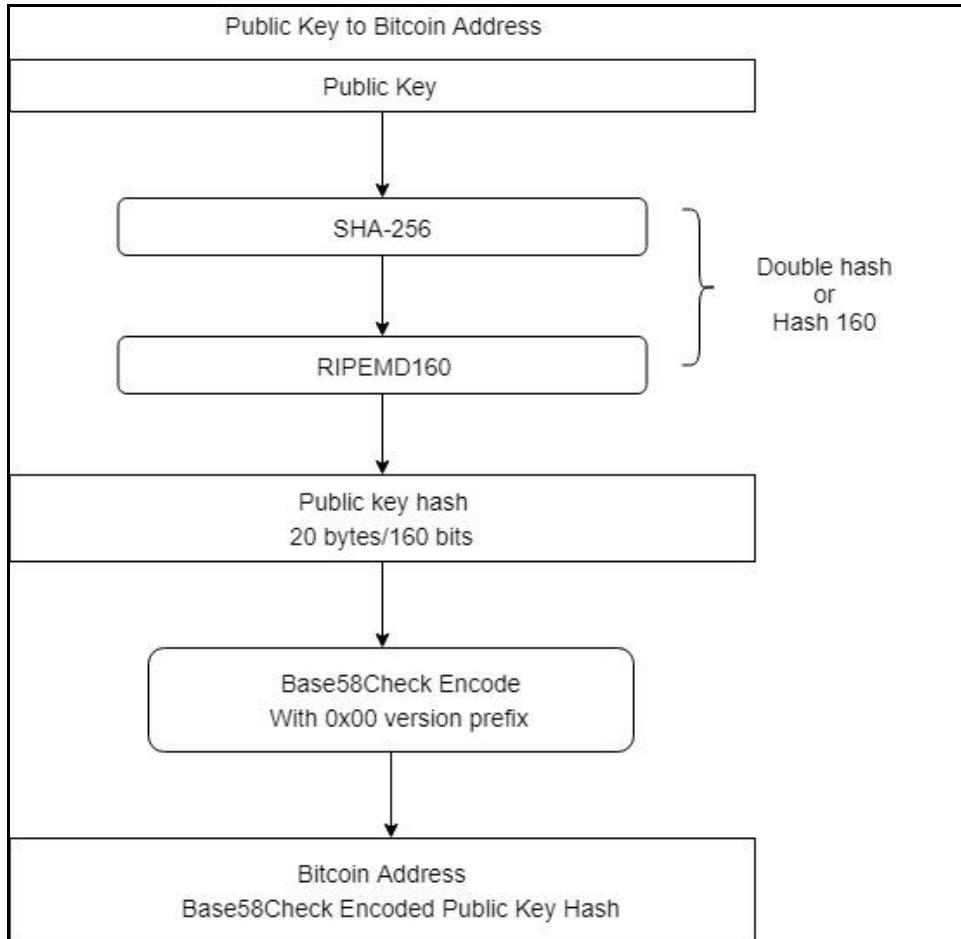
Pada Tugas Akhir ini metode keamanan sistem e-voting menggunakan teknologi blockchain yang ingin dicapai mencakup *Accuracy, invulnerability, privacy, dan verifiability*.

2.2.3 Bitcoin

Bitcoin adalah salah satu dari implementasi pertama dari *cryptocurrency* (mata uang kripto). Bitcoin mengandalkan pada jumlah pemindahan di antara rekening publik menggunakan kriptografi kunci publik (*bitcoin address*). Kunci publik atau *bitcoin address* berguna untuk mengirim atau menerima untuk semua transaksi pemindahan mata uang digital. Bitcon *address* tidak mengandung informasi apapun mengenai pemiliknya dan secara umum tidak diketahui. Bitcoin address terdiri dari format angka–angka acak dan huruf yang panjangnya sekitar 33 karakter dalam format semi numerik yang dapat dibaca.

Bitcoin mengandung kunci publik atau alamat dari pemiliknya. Misalnya ketika pengguna A mengirim suatu transaksi ke pengguna B, A akan melepaskan nilai kepemilikan mereka dengan menambahkan kunci publik atau alamat B ke koin–koin tersebut dan menandatanganinya dengan menggunakan kunci pribadi dia sendiri. Kemudian A akan menyiaran bitcoin-bitcoin ini dalam sebuah pesan atau transaksi di dalam jaringan *peer to peer*.

Untuk menyiaran sebuah transaksi atau pesan di blockchain, voter membutuhkan bitcoin address. *Broadcast* adalah proses pengiriman transaksi/pesan ke beberapa perangkat komputer lainnya secara bersamaan. Dengan menggunakan SHA256, RIPEMD160 Hashing dan Encoding Base58, bitcoin address dapat *digenerate* seperti Gambar 2.4 berikut :



Gambar 2.4. Metode generate dari public key ke bitcoin address [25]

Bitcoin menggunakan *public key* dan *private key* untuk menandatangani transaksi. Ukuran dari *private key* bitcoin adalah 256 bits. Pengguna menggunakan kunci ini untuk menandatangani transaksi setiap kali mereka mentransfer bitcoin. Karena kunci memiliki ukuran sebesar 2^{256} bit dari ruang sampel sangat tidak mungkin untuk berpotongan dengan kunci pribadi lainnya. Kunci publik berasal dari kunci privat melalui sebuah algoritma ECC (Elliptic Curve Crypto) bernama secp256k1. Kunci publik adalah pasangan (x,y) yaitu pasangan kunci untuk enkripsi (*public key*) dan deskripsi (*private key*) yang dihasilkan dari persamaan secp256k1. Keunikan kunci publik dijamin oleh keunikan kunci pribadi. Hash kunci publik dibuat menggunakan algoritma hashing SHA-256 dan RIPEMD160 seperti yang ditunjukkan pada gambar 5. Sidik jari dari sebuah kunci publik sebagai hash kunci publik memiliki ukuran 160 bits. Kunci publik adalah Base58Check diencode untuk menghasilkan bitcoin address. Alamat ini dihasilkan dari sebuah kunci

pribadi yang tidak mengandung informasi rahasia, alamat dapat diketahui oleh publik [25].

2.2.4 API (Application Programming Interface) Blockchain

API (*Application Programming Interface*) adalah sekumpulan perintah atau fungsi berupa kode program yang dapat digunakan untuk berinteraksi dengan sistem operasi tertentu atau dengan sistem lainnya. Sebuah API dapat diimplementasikan dengan membuat program yang menyediakan sarana untuk meminta layanan program tersebut.

Interface pada *software* digunakan untuk mengakses seluruh resources yang terdapat dalam software tersebut. Dengan adanya API maka akan terlihat bagaimana suatu sistem berinteraksi dengan sistem lainnya untuk mengakses *resources* melalui *interfaces* yang disediakan. Tujuan penggunaan API adalah untuk mempercepat proses *development* dengan menyediakan *function* secara terpisah sehingga developer tidak perlu membuat fitur yang sama [31].

Secara *structural* API terbentuk dari data *structure*, *object*, *function*, dan parameter-parameter yang digunakan untuk mengakses resource tersebut dari software. Seluruh spesifikasi tersebut membentuk *interface* yang dimiliki oleh *software* untuk berinteraksi dengan *software* lainnya, dan API dapat digunakan dengan berbagai bahasa programming ataupun dengan menggunakan URL yang telah disediakan suatu website. Dalam pembangunan sistem e-voting menggunakan teknologi blockchain dibutuhkan API untuk mempercepat proses *development* sistem e-voting. Salah satu API Blockchain yang dapat digunakan adalah API SoChain. API SoChain adalah layanan yang digunakan untuk membuat dan mengambil transaksi voting pada testnet bitcoin berdasarkan bitcoin address. Transaksi diambil dan ditandatangani dalam format hex dan mengirimkannya ke jaringan yang ditentukan menggunakan metode POST. Representasi hex dari transaksi berupa objek JSON.

2.3 Sistem Terdistribusi

Sistem terdistribusi adalah suatu sistem (*hardware* dan *software*) yang terdiri atas kumpulan dari komponen yang saling terhubung dan terlihat bagi pengguna sistem sebagai suatu sistem koheren tunggal. Sistem terdistribusi selalu terdiri dari

komponen independen (komputer, server, disket, printer, dan lain-lain) [18]. Sistem ini melibatkan lebih dari satu komputer dalam suatu jaringan baik lokal, internet bahkan wireless. Pada sistem e-voting yang akan dibangun komponen yang dimaksud terdiri dari kumpulan node yang saling terhubung dalam jaringan terdistribusi. Node tersebut saling berkomunikasi untuk pengiriman hasil voting ke semua node yang terhubung. Sistem Terdistribusi diatur oleh Middleware yang mampu mendistribusikan informasi pada setiap aplikasi dan antar komputer melalui jaringan. Oleh sebab itu jika ada satu komponen yang rusak, maka data dapat melewati komponen lain dan tetap bisa sampai di tujuan pada jaringan terdistribusi.

Sistem terdistribusi memiliki beberapa tujuan yaitu : berbagi resources, menjaga transparansi resources dan data, terbuka bagi sistem lain selama sistem lain memenuhi standar pada sistem terdistribusi, dan sistem terdistribusi dapat diperluas sesuai dengan kebutuhan [16].

2.4 Fungsi Hash

Fungsi hash merupakan salah satu fungsi kriptografi untuk melakukan verifikasi dan autentikasi karena fungsi ini menghasilkan nilai yang unik untuk setiap input [17]. Fungsi hash akan menghasilkan keluaran yang sama untuk tiap masukkan yang sama. Fungsi hash pada dasarnya bekerja satu arah, jika pesan diubah menjadi *message digest* maka tidak dapat lagi dikembalikan menjadi pesan semula (*irreversible*). Dengan begitu fungsi hash dapat melakukan pengecekan terhadap keaslian suatu pesan [18].

Proses autentikasi file melalui pemanfaatan nilai hash dilakukan dengan cara membandingkan nilai hash dari kedua file. Apabila nilai hash yang didapat dari kedua file adalah sama, maka file tersebut dapat dipastikan keutuhan dan autentikasinya, sedangkan jika nilai hash yang diperoleh dari kedua file tersebut berbeda maka dapat dipastikan bahwa file yang diterima tidak utuh atau telah dimanipulasi. Algoritma ini digunakan dalam berbagai aplikasi untuk autentikasi password, autentikasi keaslian file, tanda tangan digital, dan sebagainya.

Fungsi *hash* satu arah berfungsi mengoperasikan data dengan bersifat *random* dan mengubahnya menjadi nilai hash berukuran tetap (fixed). Jika ditulis dalam notasi matematika misalkan panjang pesan semula yang sifatnya sembarang

dilambangkan $H(M)$, dan panjang nilai hash yang bersifat tetap dilambangkan dengan h maka [22]:

$$h = H(M) \quad (1)$$

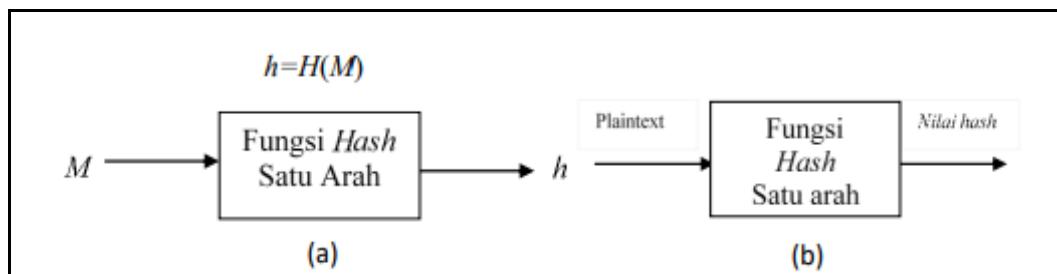
Keterangan :

H : Fungsi Hash

M : Pesan (message) yang akan diubah menjadi nilai hash

H : Nilai hash

Tidak mudah untuk mengubah masukan yang panjangnya sembarangan menghasilkan keluaran nilai hash yang mempunyai panjang yang tetap. Fungsi hash satu arah dibangun dengan fungsi kompresi, dimana masukannya adalah blok pesan dan keluaran dari blok teks atau nilai hash sebelumnya. Seperti pada Gambar 2.5 berikut ini :



Gambar 2.5. Fungsi Hash Satu Arah [19]

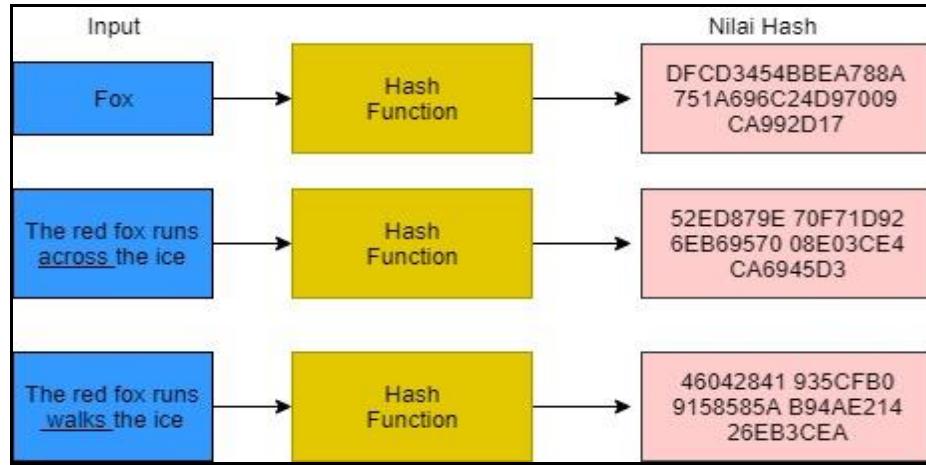
Pada gambar (a) dapat dilihat bahwa hash value dihasilkan dari pesan M yang diproses dengan fungsi hash dimana fungsinya adalah $h = H(M)$. Gambar (b) merupakan fungsi hash sederhana mengubah plaintext menjadi hash value [19].

2.5 SHA (Secured Hash Algorithm)

Pada bulan Agustus 1991, NIST (*The National Institute of Standard and Technology*) mengumumkan standart untuk tanda tangan digital yang dinamakan *Digital Signature Standart* (DSS). DSS terdiri dari dua komponen yaitu algoritma tanda-tangan digital yang disebut *Digital Signature Algorithm* (DSA) dan fungsi hash standart yang disebut *Secure Hash Algorithm* (SHA). Saat ini SHA sudah memiliki 4 versi yaitu SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, dan SHA-512. Varian SHA-0 dikenal dengan SHA-0 pada tahun 1991, varian SHA-1 dikenal dengan SHA-1 pada tahun 1993, varian SHA-224, SHA-256, SHA-384, dan SHA-512 dikenal dengan SHA-2 pada tahun 2000 [20].

SHA adalah fungsi hash yang dibuat oleh NIST dan dipublikasikan sebagai Federal Information Processing Standards (FIPS 180) pada tahun 1993. SHA adalah standard fungsi hash satu arah untuk menghitung nilai hash dari sebuah pesan atau file. Nilai hash yang dihasilkan tidak dapat diubah kembali menjadi pesan semula, sehingga disebut sebagai fungsi hash searah. Algoritma SHA-1 dapat menerima masukan maksimal sepanjang 2^{64} bit dan menghasilkan keluaran yang disebut *message digest* atau *hash code* sepanjang 160 bit. Message digest atau hash code tersebut dapat digunakan sebagai masukan untuk *Digital Signature Algorithm* (DSA) yang digunakan untuk menghasilkan signature untuk memverifikasi pesan tersebut. Pada umumnya algoritma SHA dapat dikatakan aman karena proses perhitungannya tidak memungkinkan untuk menemukan pesan yang sebenarnya dari message digest yang dihasilkan [21].

Algoritma SHA dikatakan aman karena tidak mungkin secara komputasional untuk menemukan pesan yang berpasangan dengan sebuah *message digest* tertentu. Selain itu, tidak mungkin juga secara komputasional untuk menghasilkan *message digest* yang sama. Setiap perubahan yang terjadi pada pesan akan menghasilkan *message digest* yang berbeda. Algoritma SHA memiliki perbedaan pada ukuran tiap blok, ukuran dari word yang digunakan pada saat proses hashing, panjang pesan yang dapat diproses, dan ukuran dari *message digest* yang dihasilkan berbeda-beda sesuai dengan algoritma yang dipakai. Kompleksitas algoritma dapat ditingkatkan dengan menambah jumlah *loop* yang dilakukan, menggunakan panjang data yang lebih panjang, dan menggunakan output *message digest* yang lebih panjang. Keamanan algoritma SHA dapat dibuktikan dengan *avalanche effect*, yaitu jika terjadi perubahan sedikit pada pesan, maka *message digest* yang dihasilkan dapat jauh berbeda [22]. Untuk lebih jelasnya, *avalanche effect* dapat dilihat pada Gambar 2.6 berikut :



Gambar 2.6. Avalanche Effect [22]

Algoritma SHA terdiri dari dua tahap yaitu *preprocessing* dan proses hash atau message digest. *Preprocessing* terdiri dari *padding* pesan (penambahan bit pengganjal), *parsing* pesan (membagi pesan menjadi blok-blok dengan panjang tertentu), dan menginisialisasi nilai awal dari *message digest* sebelum dilakukan perhitungan *message digest*. Sedangkan proses hash menghasilkan persiapan *message schedule*, *initialize variable*, komputasi SHA-256, dan menjumlahkan *variable*.

SHA membutuhkan 5 buah penyangga (*buffer*) yang masing-masing panjangnya 32 bit. Total panjang penyangga adalah 160 bit. Kelima penyangga ini diberi nama A,B,C,D, dan E. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut :

$$A = 67452301$$

$$B = EFCDAB89$$

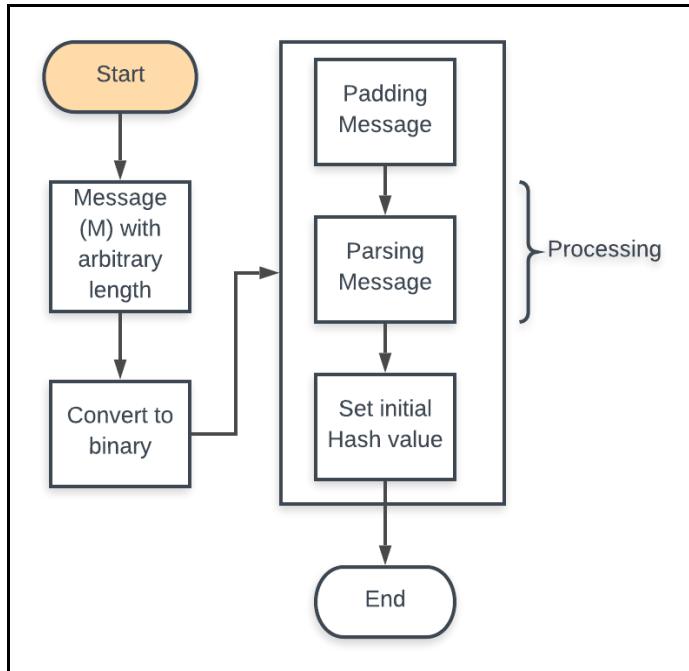
$$C = 98BADCFE$$

$$D = 10325476$$

$$E = C3D2E1F0$$

Proses SHA terdiri dari 4 *round* yang mempunyai 80 operasi. Dengan demikian, untuk memproses setiap satu blok pesan 512 bit diperlukan 80 operasi .

Berikut Gambar 2.7 Tahap *preprocessing* pada SHA adalah sebagai berikut :



Gambar 2.7. Tahap Processing pada SHA

Tahapan yang dilakukan pada preprocessing adalah sebagai berikut :

1. *Padding* Pesan

Pada tahap ini, pesan yang berupa binary disisipkan dengan angka 1 dan ditambahkan bit-bit pengganjal yakni angka 0 hingga panjang pesan tersebut kongruen dengan 448 modulo 512. Panjang pesan yang asli kemudian ditambahkan sebagai angka biner 64 bit maka panjang pesan sekarang menjadi kelipatan 512 bit.

2. *Parsing* Pesan

Parsing pesan merupakan proses membentuk blok-blok pesan yang masing-masing memiliki 512 bit. Kemudian masing-masing blok 512 bit dikelompokkan ke dalam 16 blok pesan yang masing-masing bloknya terdiri dari 32 bit.

3. Inisialisasi nilai hash awal

Pada SHA untuk menyimpan nilai inisialisasi awal dan nilai output sementara digunakan *buffer* H_0, H_1, H_2, H_3, H_4 . Berikut inisial hash value dalam notasi hexadesimal adalah sebagai berikut :

$$H_0 = 0x67452301$$

$$H_1 = 0xefcdab89$$

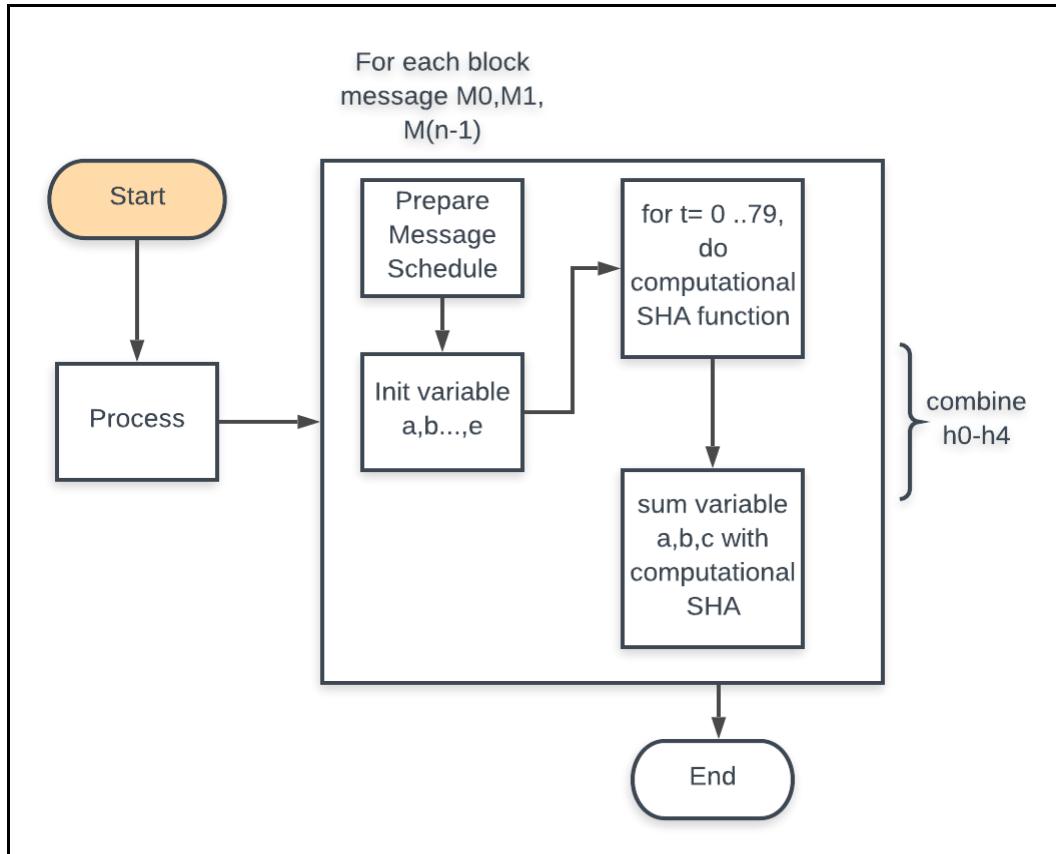
$$H_2 = 0x98BADCFE$$

$$H_3 = 0x10325476$$

$$H_4 = 0xC3D2E1F0$$

Setelah proses *preprocessing* dilakukan tahap *hash computation* pada SHA-256.

Tahap *hash computation* digambarkan seperti Gambar 2.8 berikut :



Gambar 2.8. Tahap Hash Computation pada Hash

Pada tahap *hash computation* merupakan inti dari proses ini yang terdiri dari 4 *round* yang mempunyai 80 langkah. Untuk memproses setiap satu blok pesan 512 bit diperlukan 80 operasi. Untuk setiap blok pesan dilakukan langkah-langkah berikut [23] :

1. Message Schedule
2. Inisialisasi Variable
3. Proses Komputasi
4. Menjumlahkan Variabel
5. Output

Dengan menerapkan algoritma SHA ini dapat memudahkan user untuk menyelidiki keaslian suatu file yang dimilikinya dengan file aslinya, sehingga

user dapat memastikan keotentikan atau keaslian suatu file yang dimilikinya dan terhindar dari tindakan pemalsuan atau manipulasi terhadap file oleh pihak – pihak yang tidak berwenang atas file tersebut. Pengujian untuk kedua file yang sama akan menghasilkan nilai hash yang sama pula sehingga dapat dipastikan bahwa isi file tersebut tidak dapat dimanipulasi dan merupakan file yang utuh. Sedangkan apabila nilai hash kedua file berbeda maka dapat dipastikan file tersebut berbeda atau dimanipulasi. Implementasi dari algoritma SHA ini diharapkan dapat menghindarkan tindakan manipulasi terhadap file yang akan dikirimkan [24].

2.6 Institut Teknologi Del

Institut Teknologi Del adalah salah satu perguruan tinggi swasta yang berkedudukan di desa Sitoluama, Toba Samosir, Sumatera Utara, Indonesia. IT DEL didirikan oleh Luhut Binsar Panjaitan yang merupakan Menteri Perindustrian dan Perdagangan Republik Indonesia ke-28. ITDEL mulai melakukan kegiatan akademik pada tahun 2001 dan telah menamatkan 15 angkatan hingga saat ini pada Oktober 2018. IT DEL memiliki tiga fakultas yaitu Fakultas Teknologi Informatika dan Elektro (FTIE), Fakultas Teknologi Industri (FTI), dan Fakultas Bioteknologi (FB) dengan 8 program studi yaitu Diploma 3 Teknik Informatika, Diploma 3 Teknik Komputer, Diploma 4 Teknik Informatika, S1 Teknik Informatika, S1 Teknik Elektro, S1 Sistem Informasi, S1 Manajemen Rekayasa, dan S1 Teknik Bioproses.

Saat ini IT DEL memiliki sistem informasi yaitu Campus Information System (CIS) yang digunakan oleh dosen, kemahasiswaan, baak, dan mahasiswa untuk memperoleh pengumuman baik akademik maupun non-akademik. Sistem CIS telah menyediakan menu khusus yaitu menu survey untuk melakukan polling. Kegiatan polling yang saat ini dilakukan di IT DEL pada sistem adalah pemilihan mahasiswa teladan. Polling mahasiswa teladan dilakukan oleh seluruh mahasiswa ITDEL. Pada menu polling dilengkapi dengan bagian-bagian yang terdiri dari halaman untuk melakukan polling yang dilakukan oleh pengguna polling, daftar seluruh polling yang telah dilakukan, form untuk mengelola polling, hasil polling dan hasil rekapitulasi polling. Pada menu untuk mengelola polling yaitu tambah polling terdiri dari form yang berisi judul, pertanyaan, keterangan, start polling,

polling end, polling wajib diisi oleh peserta, Opsi 1, Opsi 2, Opsi 3 Opsi n dan pengguna yang akan melakukan polling terdiri dari developer, dosen, mahasiswa, baak, pegawai, teaching-assistant, hrd, keasramaan, dan finance.

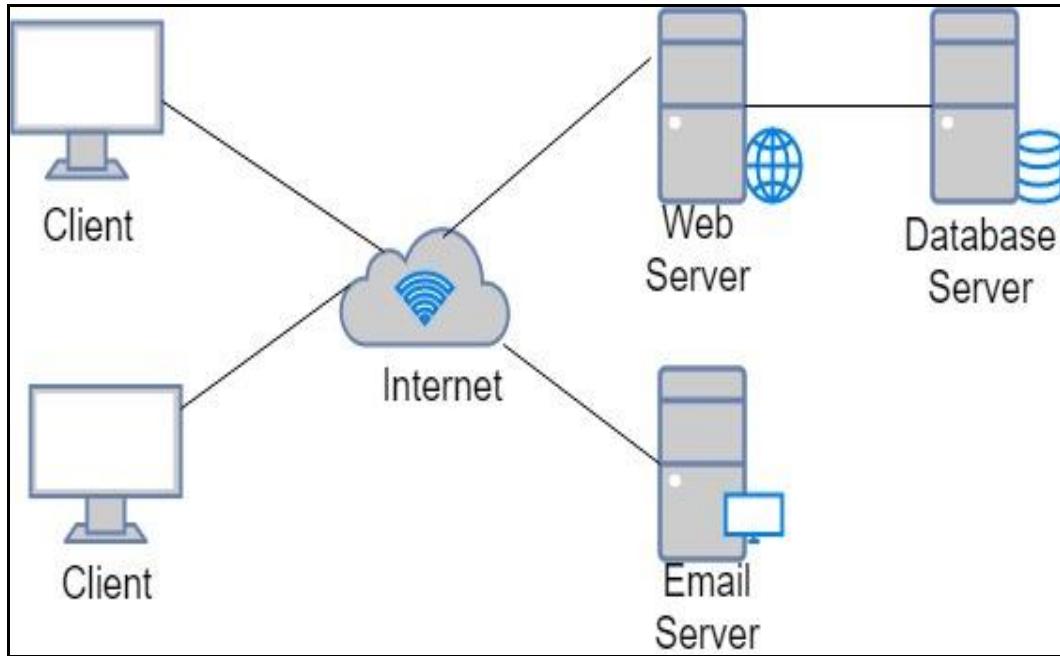
Pada rekapitulasi polling terdiri dari gambar diagram lingkaran jumlah generate voting masing-masing kandidat, sedangkan hasil polling terdiri dari opsi (informasi setiap kandidat), hasil vote, jumlah voter yang memilih masing-masing kandidat, dan total voter yang melakukan polling. Selain itu voter juga dapat mencetak hasil rekapitulasi polling dengan mendownload hasil rekapitulasi polling yang disediakan dalam berbagai ekstensi file gambar seperti *PNG image, JPEG image, PDF document, SVG vector image*.

2.7 Web Application

Web *applications* menggunakan sebuah *client-server architecture*. Arsitektur ini terdiri dari *server* yang membagikan *resources* dengan klien melalui jaringan. Berikut Gambar 10 menunjukkan komponen dari arsitektur *client server*.

Server dapat membagikan file, website, database, dan email. Sebuah server dapat berbagi websites dan sebuah web browser adalah *client software* yang digunakan untuk mengakses *web server*.

Sebuah network adalah sistem komunikasi yang mengizinkan *client* dan *server* untuk berkomunikasi. *Network* bertanggung jawab untuk mendapatkan informasi dari satu komputer dengan komputer lainnya. Proses ini disebut sebagai *routing*. Sebuah router adalah *device* yang menghubungkan dua atau lebih *networks*. Ketika informasi datang dari satu *network*, router menentukan jaringan mana yang paling dekat dengan tujuan dan mengirimkan informasi keluar pada jaringan itu [27].



Gambar 2.9. Arsitektur Web Application [27]

2.8 Database

Database adalah semua informasi yang dapat menyimpan tentang data user, dokumen, dan kebutuhan yang diperlukan dalam sistem dunia nyata yang dipetakan ke table, kolom, baris dari database. Setiap tabel mempresentasikan satu objek atau entity pada system. Kemudian dalam setiap tabel, kolom menyimpan satu item dari informasi atau attribute untuk entity, dan setiap baris menyimpan satu kejadian atau contoh dari entity. Untuk memodelkan sebuah database dan hubungan di antara tabel kita dapat menggunakan teknik entity-relationship (ER) modelling [27].

2.8.1 MySQL

MySQL dikembangkan sekitar tahun 1994 oleh sebuah perusahaan pengembang software dan konsultan database bernama MySQL AB yang bertempat di Swedia. MySQL adalah Relational Database Management Sistem (RDBMS) secara gratis dibawah GOL (General Public Lisence). Setiap orang bebas menggunakan MySQL namun tidak untuk dijadikan produk turunan yang bersifat komersial. MySQL merupakan SQL (Structure Query Language).

SQL adalah konsep pengoperasian database, terutama untuk pemilihan atau pemasukan data yang memungkinkan dikerjakan dengan mudah dan otomatis.

MySQL dapat dikatakan lebih unggul dibandingkan database server lainnya dalam query data. Kecepatan query bisa sepuluh kali lebih cepat dari PostgreSQL dan lebih cepat dibandingkan dengan interbase. Jadi MySQL adalah satu dari sekian banyak sistem database yang didukung oleh ribuan komunitas pengguna di internet [28].

2.8.2 Bahasa Pemograman yang Didukung

Pada implementasi penulis menggunakan javascript dan PHP. Javascript adalah Bahasa script objek yang mudah digunakan untuk membuat aplikasi online yang menghubungkan objek dan resources pada kedua clients dan servers. Javascript adalah design yang digunakan oleh authors development pada HTML. Design dan konsep representasi java script oleh software internet yaitu sebagai berikut [29] :

1. Dirancang untuk membuat aplikasi berbasis jaringan
2. Terintegrasi dengan java
3. Terintegrasi dengan HTML
4. Platform terbuka

PHP (atau resminya PHP: Hypertext Preprocessor) adalah skrip berbasis server side yang ditambahkan kedalam HTML. PHP sendiri merupakan singkatan dari Personal Home Page tools. Server side berarti pengerjaan skrip akan dilakukan di server, kemudian hasilnya dikirimkan ke browser.

Keunggulan dari server-side adalah tidak diperlukan kompatibilitas browser karena serverlah yang akan mengerjakan skrip PHP sehingga hasil yang dikirimkan browser bersifat teks dan gambar, dapat memanfaatkan sumber-sumber aplikasi lain seperti koneksi ke database, dan skrip tidak dapat “diintip” dengan menggunakan fasilitas view HTML source [30] .

2.9 Related Works

Berikut merupakan daftar dari *related work* atau penelitian yang telah dilakukan sebelumnya. Dari daftar penelitian ini dapat diketahui bagaimana beberapa teknologi blockchain telah digunakan oleh berbagai aplikasi seperti keuangan, e-voting, dan lain-lain.

Tabel 2.1. Related Works

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
1	<i>Blockchain-Based E-Voting System</i>	Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson	2018	Kerangka kerja yang diterapkan kontrak cerdas pemilihan adalah Exonum, Quorum, dan Geth	algoritma konsensus bukti-otoritas (POA)	Paper ini bertujuan membangun sistem pemungutan suara elektronik dan mengidentifikasi keterbatasan hukum dan teknologi menggunakan blockchain sebagai layanan untuk mewujudkan sistem tersebut. Sistem ini dimulai dengan mengidentifikasi peran dan komponen untuk menerapkan smart	Hasil penelitian menunjukkan dengan memperkenalkan sistem e-voting menggunakan smart contract untuk memungkinkan pemilihan yang aman dan hemat biaya Penulis telah menguraikan arsitektur sistem, desain, dan analisis keamanan sistem. Dibandingkan dengan pekerjaan sebelumnya, penulis telah menunjukkan bahwa teknologi blockchain menawarkan kemungkinan baru bagi negara demokratis untuk maju dari skema pemilihan menggunakan pena dan kertas, ke skema pemilihan waktu yang

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
						contract e-voting, kemudian mengevaluasi kerangka kerja berbeda yang dapat digunakan untuk merealisasikan dan menyebarkan kontrak cerdas pemilihan. Sistem yang dirancang menggunakan otentifikasi ID elektronik melalui Auðkenni.	efisien. Future Works : Menggunakan blockchain Ethereum untuk mengirimkan ratusan transaksi per detik ke blockchain
2	<i>Perancangan dan Implementasi Sistem Pencatatan E-Voting Berbasis Blockchain</i>	Rifa Hanifatunissa	2017	Simulasi menggunakan Bahasa pemograman Phyton .	-	Penelitian dimulai dengan membuat latar belakang dan identifikasi masalah yang terjadi pada sistem pemilu konvensional, mendefinisikan tujuan, batasan rancangan implementasi,	Sistem ini berhasil secara fungsionalitas melakukan pencatatan sistem e-voting berbasis teknologi blockchain. Sistem ini menggunakan Protocol Permission untuk sistem pencatatan terdistrbusi dengan pengoperasian dilakukan oleh entitas yang dikenal pengoperasian dilakukan oleh entitas yang

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
						<p>desain sistem, melakukan implementasi dan pengujian, melakukan analisis dan evaluasi, dan pembuatan laporan dan seminar.</p> <p>Proses ini dimulai ketika proses pemungutan suara telah selesai. Sebelum proses pemilihan dimulai, setiap node menghasilkan private key dan public key. Public key masing-masing node dikirim ke semua node yang tercantum dalam proses pemilihan. Ketika pemilihan terjadi, setiap simpul mengumpulkan</p>	<p>dikenal, dengan kata lain memiliki sarana untuk mengidentifikasi node yang dapat mengendalikan dan memperbarui data bersama dalam mencapai tujuan kepercayaan dari partisipan. Entitas yang dikenal dalam sistem ini adalah setiap node yang telah terdaftar sebelum proses berjalan, dengan public key pada setiap node dimiliki daftarnya oleh seluruh node dalam sistem. Pada pengujian secara non-fungsional didapatkan hasil bahwa sistem yang diimplementasikan dengan Bahasa pemrograman Python mampu menangani keseluruhan proses pencatatan sistem e-voting ini dengan waktu rata-rata yang dibutuhkan setiap node dalam membuat block adalah 0.24 detik dan rata-rata kapasitas yang dibutuhkan untuk</p>

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
						<p>hasil pemilihan dari masing-masing pemilih. Ketika proses seleksi selesai, node akan menunggu giliran untuk membuat blok. Setelah kedatangan blok di setiap node, kemudian dilakukan verifikasi untuk menentukan apakah blok tersebut valid. Setelah valid, maka database ditambahkan dengan data di blok tersebut. Setelah pembaruan basis data, node akan memeriksa apakah ID node yang dibawa sebagai token</p>	<p>menyimpan data sebesar 216.04 Bytes untuk setiap blok.</p> <p>Future Work : Pengujian antar perangkat dilakukan dengan menggunakan jaringan internet untuk setiap node agar hasil penelitiannya dapat lebih menggambarkan implementasi real.</p>

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
						<p>adalah miliknya atau tidak. Jika node mendapat giliran, itu akan membuat dan mengirimkan blok yang telah diisi dengan tanda tangan digital untuk disiarkan ke semua node dengan menggunakan aturan giliran dalam pembuatan blockchain untuk menghindari tabrakan dan memastikan bahwa semua node dalam blockchain. Blok yang dikirimkan berisi id node, id node selanjutnya seperti yang digunakan sebagai token, timestamp, hasil</p>	

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
						voting, hash dari node sebelumnya, dan digital tanda tangan dari node.	
3	<i>E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy</i>	Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis	2018	-	-	Jurnal ini mengeksplorasi potensi teknologi blockchain dan kegunaannya dalam skema e-voting. Tiga protokol e-voting yang paling terdokumentasi dan popular yaitu BitCongress, Follow my Vote, dan TIVI. Protokol voting yang diusulkan menggunakan blockchain untuk menyimpan suara dimana blockchain bertindak sebagai kotak suara transparan. Untuk	Jurnal ini menyoroti beberapa kekurangan dan menyajikan dua jalur potensial ke depan untuk meningkatkan platform yang mendasari teknologi blockchain untuk mendukung e-voting dan aplikasi serupa lainnya. Diperlukan upaya terpadu dalam penelitian teknologi blockchain untuk meningkatkan fitur dan dukungan untuk aplikasi kompleks yang dapat dijalankan dalam jaringan blockchain.

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
						implementasi menggunakan jaringan pribadi yang menggunakan Ethereum blockchain API.	
4	<i>Rancang Bangun Sistem E-Voting Dengan Menggunakan Teknologi Blockchain</i>	Ade Rayendra	2017	Perangkat lunak blockchain akan dibuat dengan menggunakan Bahasa pemrograman C# dengan .Net Framework Programming	-	Pada penelitian ini beberapa metode yang digunakan yaitu analisis sistem dengan melakukan studi literatur, observasi, wawancara, perancangan sistem dan pembangunan sistem, pengujian dan implementasi. Pada penelitian ini dirancang alat e-voting atau diberi nama Voting station. Sistem ini menggunakan Raspberry Pi	Hasil dari penelitian ini adalah sistem e-voting yang telah dirancang mampu melakukan fungsi utama dengan baik, mampu memvalidasi identitas pemilih, mencegah pengulangan pemilihan, mampu menjadi penyimpanan data voting yang aman, proses pemilihan cepat dan aman, perhitungan suara lebih cepat dan memungkinkan mengaudit hasil pemilihan karena adanya jejak data yang bisa dilihat. Future Works : Menambahkan gambar untuk

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
						<p>sebagai pengontrol utama Voting-station. Proses pemilihan oleh seorang voter ditandai dengan voter menginputkan ID identitasnya kemudian voting-station akan memvalidasi kartu identitas tersebut. Setelah voting-station menyatakan bahwa identitas tersebut valid, kemudian voting-station akan menampilkan kandidat yang akan dipilih voter.</p>	<p>setiap kandidat sehingga lebih memudahkan bagi pemilih untuk memilih kandidat, meningkatkan efisiensi sistem dan kinerja pemrosesan data yang ada pada sistem.</p>
5	<i>Towards Secure E-Voting Using Ethereum Blockchain</i>	Ali Kaan Koç, Umut Can Çabuk, Emre Yavuz, Gökhan	2018	- Sistem e-voting dibangun dengan kontrak	-	<p>Paper ini membahas pembangunan sistem e-voting dengan</p>	<p>Hasil percobaan dari penelitian ini adalah dengan menggunakan kekuatan jaringan Ethereum dan struktur blockchain</p>

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
		Dalkılıç		<p>cerdas Ethereum menggunakan platform blockchain Ethereum. Kontrak cerdas ini ditulis dalam Bahasa pemograman Soliditas yang merupakan kombinasi dari C ++ dan JavaScript.</p> <ul style="list-style-type: none"> - Platform Ethereum didukung di Linux, OS X, dan platform Window. - Memiliki koin Ethereum untuk mengeksekusi aplikasi dan 		<p>menggunakan platform blockchain Ethereum untuk jenis pemilu skala kecil. Contoh platform Ethereum adalah kontrak cerdas. Kontrak pintar adalah potongan kode yang berarti, untuk diintegrasikan dalam blockchain dan dijalankan sesuai jadwal di setiap langkah pembaruan blockchain. Blockchain dengan kontrak cerdas, muncul sebagai kandidat yang baik untuk digunakan dalam pengembangan sistem e-voting yang lebih aman,</p>	<p>metodologi keamanan yang digunakannya, yaitu rantai hash yang tidak dapat diubah, telah menjadi dapat beradaptasi dengan jajak pendapat dan pemilihan. solusi e-voting berbasis-blockchain, termasuk yang telah kami terapkan menggunakan kontrak cerdas dan jaringan Ethereum, alamat (atau mungkin alamat dengan modifikasi yang relevan) hampir semua masalah keamanan, seperti privasi pemilih, integritas, verifikasi dan non-penolakan suara, dan transparansi penghitungan. Namun sistem ini masih terbatas untuk pemilihan skala kecil. Skalabilitas jaringan Ethereum masih belum diketahui dan perlu penelitian lebih lanjut, itu sebabnya penulis tidak dapat menyarankan penggunaan kontrak ini untuk pemilihan</p>

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
				memberikan suara		<p>lebih murah, lebih aman, lebih transparan, dan lebih mudah digunakan. Ethereum dan jaringannya adalah salah satu yang paling sesuai, karena konsistensinya, penggunaan yang luas, dan ketentuan logika kontrak cerdas. Tujuan paper ini adalah membangun aplikasi e-voting sebagai kontrak cerdas dengan jaringan Ethereum menggunakan dompet Ethereum dan bahasa Soliditas. Penulis membangun kontak cerdas Ethereum dalam</p>	<p>nasional, setidaknya untuk saat ini. Kontrak smart yang dibangun penulis dijalankan di blockchain Ethereum, jadi di mana pun dompet Ethereum dapat dijalankan (lokasi, platform, perangkat, dll.). Aplikasi voting penulis juga dapat digunakan.</p>

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
						<p>skala kecil untuk membuat proses pemilihan universitas penulis online. Untuk membangun sistem ini penulis terlebih dahulu mendefinisikan kontrak pintar. Kontrak-kontrak ini ditulis dalam bahasa pemrograman Soliditas, yang merupakan kombinasi dari C++ dan JavaScript. Kontrak pintar dijalankan oleh rekan-rekan dari jaringan Ethereum di setiap 15 detik, dan mereka harus divalidasi setidaknya oleh 2 pengguna lain</p>	

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
						untuk diaktifkan. Setelah itu, fungsi kontrak dapat dijalankan, dan kontrak dapat dibagi dengan kandidat lain. Penulis mendefinisikan struct dan variable pemilih dan mengumpulkan pemilih dalam suatu larik, membuat blok kode dari fungsi yang menginisialisasi pemilih, blok kode yang mendefinisikan proses pengecoran suara, blok kode mengembalikan hasil pemungutan suara.	
6	Electronic Voting	Kibin Lee, Joshua	2016	Dalam jurnal ini	-	Dalam pekerjaan ini kita membahas	Dalam karya ini, penulis memperkenalkan sistem

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
	Service Using Block-Chain	I.James, Tekachew G. Ejeta, Hyoung J. Kim		memperkenalkan sistem pemungutan suara elektronik yang menggunakan Block-chain sebagai buku besar transaksi, dimana otentikasi dan penyaringan dilakukan oleh otentikasi organisasi dan pihak ketiga yang terpercaya. Dengan sistem yang diusulkan pemilih harus mengidentifikasi hak mereka untuk		kriteria pemilihan elektronik, dan bagaimana block-chain dapat digunakan sebagai metode yang transparan dan hemat biaya untuk mengelola dan memverifikasi transaksi dalam pemungutan suara skala besar. Bitcoin address, dan khususnya blok-rantai, dapat digunakan untuk memantau dan memverifikasi transaksi. Pada jurnal ini mengusulkan kriteria pemilihan elektronik, yang meliputi: integritas sistem, integritas dan keandalan data, anonimitas	pemungutan suara elektronik yang menggunakan Block-chain sebagai buku besar transaksi, dimana otentikasi dan penyaringan dilakukan oleh otentikasi organisasi dan pihak ketiga yang terpercaya. Informasi transaksi disimpan dalam block-chain yang dapat digunakan untuk mengaudit integritas transaksi, Fokus pada jurnal ini adalah potensi ketersediaan teknologi rantai blok untuk penggunaan transaksional lainnya. Block-chain adalah salah satunya buku besar terbuka paling stabil yang menjaga informasi transaksi, dan sulit dipalsukan. Sejak informasi yang disimpan dalam blok-rantai tidak terkait dengan informasi pengenal pribadi, yang dimilikinya karakteristik anonimitas. Juga, block-chain memungkinkan untuk

No	Judul	Author	Tahun	Output	Algoritma	Tahap Pengerjaan	Kesimpulan
				memilih dengan membuktikan diri mereka pada organisasi yang mengontektasi dan TTP. Kemudian dengan menerbitkan kedua sisi daftar, pemilih tahu bahwa suara yang diberikan secara unik divalidasi dan diaudit		dan data pemilih kerahasiaan, dan otentikasi operator. Ada empat bagian yang terlibat dalam model pemilihan elektronik ini yaitu organization, trusted third party, voters, dan block-chain	transaksi transparan verifikasi karena semua informasi dalam rantai blok terbuka untuk umum. Karakteristik ini adalah sama dengan persyaratan untuk sistem pemungutan suara. Yaitu, ketahanan yang kuat, anonimitas, dan transparansi. Dalam makalah ini, kami mengusulkan sistem pemungutan suara elektronik sebagai aplikasi rantai-blok, dan menjelaskan pemungutan suara berbasis rantai-blok di tingkat nasional melalui contoh-contoh.

2.10 Kesimpulan

Berdasarkan hasil tinjauan pustaka dapat disimpulkan beberapa hal yang menjadi acuan dalam desain, implementasi, dan pengujian adalah sebagai berikut:

1. Pembangunan sistem e-voting memanfaatkan teknologi blockchain dengan hasil data pemilu tereplikasi ke semua node yang terlibat dalam jaringan blockchain.
2. Dengan menggunakan teknologi blockchain pada sistem e-voting tidak satupun yang mengetahui identitas pemilih dan data yang dipilih oleh voter.
3. Dengan menggunakan teknologi blockchain pada sistem e-voting penyimpanan transaksi voting, proses pemilihan, perhitungan suara menjadi aman.
4. Untuk membangun sistem e-voting menggunakan teknologi blockchain penulis menggunakan framework yii2 dengan bahasa pemrograman PHP, Javascript, framework yii2 dan API Blockchain yang digunakan sebagai layanan untuk membuat dan mengambil transaksi voting adalah API SoChain.
5. Dengan menggunakan API SoChain siapapun yang terlibat dalam jaringan blockchain dapat melihat dan menghitung transaksi voting pada bitcoin tesnet.
6. Algoritma SHA digunakan untuk hashing transaksi dan sudah menjadi ketentuan pada blockchain jika ingin membuat transaksi.

BAB 3

ANALISIS

Pada bab analisis berisi uraian mengenai pengenalan proyek, *project plan*, dan analisis yang dilakukan terhadap sistem yang masih berjalan saat ini untuk mendapatkan rancangan aplikasi yang akan dikembangkan.

3.1 Pengenalan Proyek

Institut Teknologi Del merupakan studi kasus dari pembangunan sistem informasi ini. Sistem yang akan dibangun adalah Sistem E-Voting menggunakan teknologi blockchain berbasis web. Pengerjaan sistem ini mencakup kegiatan e-voting di kampus.

3.2 Project Plan

Berikut ini akan dijelaskan bagaimana *developer* membangun sistem e-voting menggunakan teknologi blockchain :

1. Sistem yang akan dibangun dimulai dengan tahapan menentukan topik, perumusan masalah, studi pustaka, desain, analisis, implementasi, pengujian, hasil dan pembahasan, dan kesimpulan.
2. Kelompok yang beranggotakan dua orang akan mengerjakan aplikasi web.
3. Untuk memanajemen waktu maka developer membuat *schedule* tahap pengerjaan setiap minggunya.
4. Melakukan bimbingan dengan pembimbing mengenai sistem yang akan dibangun.
5. Melakukan observasi di Institut Teknologi Del untuk melakukan *requirement gathering*.

3.3 Pengumpulan Data

Pada subbab ini akan dijelaskan mengenai pengumpulan data yang dilakukan di Institut Teknologi Del yang akan menjadi pengguna sistem. Berikut akan dijelaskan tahapan dalam pengumpulan data.

3.3.1 Persiapan Survei

Pada bagian ini akan dijelaskan mengenai persiapan survey yang dilakukan. Pada survei ini dilakukan di Institut Teknologi Del. Teknik yang dipilih dalam

melakukan survei yaitu observasi. Observasi merupakan teknik pengumpulan data dengan pengamatan langsung dan pencatatan secara sistematis terhadap objek yang akan diteliti. Sebelum melakukan survei adapun persiapan yang dilakukan yaitu melakukan survei di internet terlebih dahulu terkait dengan hal yang dipermasalahkan untuk memperoleh informasi awal sebagai bahan untuk melakukan survei.

3.3.2 Pelaksanaan Survei

Pada bagian ini akan dijelaskan mengenai pelaksanaan survei yang dilakukan. Pelaksanaan survei yang dilakukan adalah melakukan pengamatan dengan sistem e-voting yang masih berjalan saat ini di Institut Teknologi Del. Developer mengamati dari proses login ke sistem sampai melakukan vote oleh voter (mahasiswa) serta bagaimana sistem menampilkan hasil rekapitulasi polling dan proses mengelola polling oleh admin. Sistem yang digunakan oleh voter untuk melakukan voting adalah CIS (*Campus Information System*). CIS merupakan sistem yang dimanfaatkan oleh dosen, kemahasiswaan, baak, dan mahasiswa untuk memperoleh pengumuman baik akademik maupun non-akademik. Sistem CIS telah menyediakan menu khusus yaitu menu survey untuk mengakses polling. Admin dapat mengelola polling apapun terkait permasalahan akademik dan non-akademik. Voter yang akan melakukan vote yaitu tergantung kepada pengguna yang ditujukan untuk melakukan voting. Untuk pengolahan hasil voting mencakup masing-masing pilihan voter, perhitungan suara, dan cara mendapatkan suara dilakukan di satu *server* khusus milik Institut Teknologi Del. Setiap orang tidak sembarangan untuk mengakses *server* ini, hanya orang yang telah memiliki hak akses khusus yang dapat mengakses sistem ini.

3.3.3 Hasil Survei

Adapun hasil yang didapatkan setelah melakukan survei adalah sebagai berikut :

1. *Developer* mengetahui sistem yang digunakan sebagai kegiatan polling di Institut Teknologi Del.
2. *Developer* mengetahui bagaimana alur atau bisnis proses mulai dari login ke sistem sampai melakukan vote.

3. *Developer* mengetahui bagaimana sistem polling yang berjalan saat ini (*current system*) di Institut Teknologi Del.

3.4 Analisis Sistem Polling

Sistem polling merupakan sistem yang digunakan untuk melakukan kegiatan polling di Institut Teknologi Del. Sistem yang digunakan untuk melakukan voting adalah CIS (*Campus Information System*). CIS telah menyediakan modul polling yaitu menu survey untuk mengakses polling.

Pada menu polling dilengkapi dengan bagian-bagian yang terdiri dari daftar seluruh polling yang telah dilakukan, form untuk mengelola polling, dan hasil rekapitulasi polling. Pada menu untuk mengelola polling yaitu tambah polling terdiri dari form yang berisi judul, pertanyaan, keterangan, start polling, polling end, polling wajib diisi oleh peserta, Opsi 1, Opsi 2, Opsi 3 Opsi n dan pengguna yang akan melakukan polling terdiri dari developer, dosen, mahasiswa, baak, pegawai, teaching-assistant, hrd, keasramaan, dan finance.

Pada rekapitulasi polling terdiri dari gambar diagram lingkaran hasil *generate voting*, opsi (informasi setiap kandidat), hasil vote, jumlah voter, dan total voter setiap kandidat. Selain itu voter juga dapat mencetak hasil rekapitulasi polling dengan mendownload hasil rekapitulasi polling yang disediakan dalam berbagai ekstensi file gambar seperti *PNG image*, *JPEG image*, *PDF document*, *SVG vector image*.

3.5 Analisis Rekam Polling

Pada subbab berikut akan dijelaskan setiap fungsionalitas pengguna sistem polling.

a. Admin

Fungsionalitas sistem admin adalah :

1. Fungsi login

Fungsi ini digunakan untuk dapat mengakses sistem.

2. Fungsi melihat detail polling

Fungsi ini digunakan untuk melihat data polling yang pernah dilakukan oleh voter.

3. Fungsi search polling

Fungsi ini digunakan untuk mencari data polling dengan menggunakan keyword berdasarkan judul dan pertanyaan.

4. Fungsi mengelola data polling

Fungsi ini digunakan untuk menambah, mengedit, dan menghapus informasi yang berhubungan dengan daftar polling.

b. Voter

Voter pada sistem ini terdiri dari terdiri dari developer, dosen, mahasiswa, baak, pegawai, teaching-assistant, hrd, keasramaan, dan finance.

Fungsionalitas sistem voter adalah :

1. Fungsi login

Fungsi ini digunakan untuk dapat masuk ke dalam sistem.

2. Fungsi melakukan vote

Fungsi ini digunakan untuk melakukan vote pada sistem polling.

3. Fungsi melihat detail polling

Fungsi ini digunakan untuk melihat data polling yang pernah dilakukan oleh voter.

4. Fungsi search polling

Fungsi ini digunakan untuk mencari data polling dengan menggunakan keyword berdasarkan judul dan pertanyaan.

5. Fungsi mencetak rekapitulasi polling

Fungsi ini digunakan untuk mencetak hasil rekapitulasi polling setelah mendownload file.

Fitur-fitur yang tersedia pada polling :

1. Penambahan daftar polling

2. Pengeditan daftar polling

3. Penghapusan daftar polling

4. History data polling

5. List polling yang pernah dilakukan

6. Daftar kandidat

7. Informasi setiap kandidat seperti nama, prodi mahasiswa.

8. Informasi hasil rekapitulasi polling

9. Informasi hasil polling seperti hasil vote, jumlah voter setiap kandidat dan total voter yang melakukan polling
10. Informasi detail form kelola polling
11. *Download* rekapitulasi polling
12. Pencetakan rekapitulasi polling
13. Pencarian daftar polling berdasarkan judul dan pertanyaan

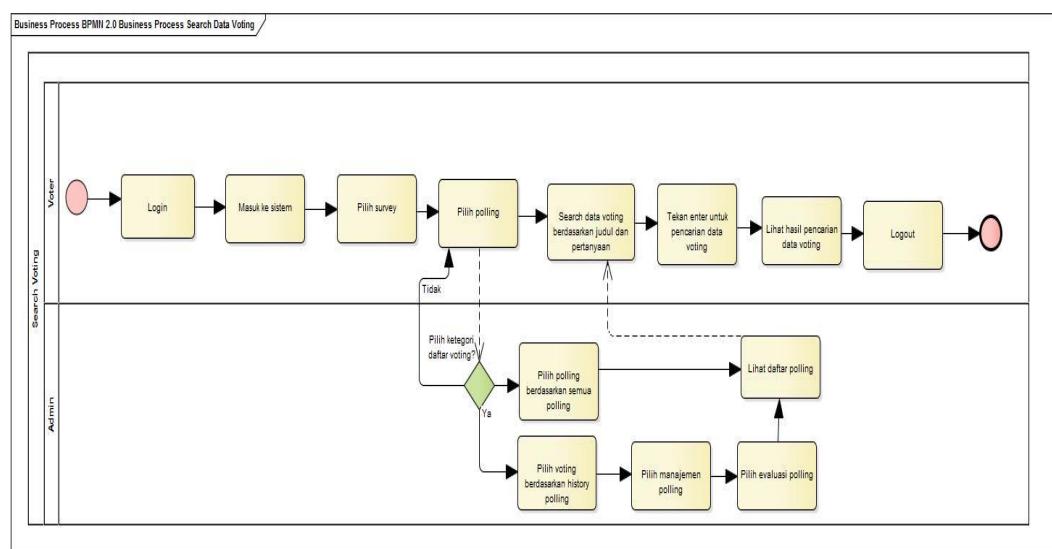
3.6 Current System

Pada subbab ini akan dijelaskan bagaimana analisis sistem polling yang masih berjalan saat ini di Institut Teknologi Del.

1. Search Data Polling

Berikut merupakan bisnis proses dari *search data polling*.

Bisnis proses oleh admin dan voter untuk *search data voting* pada *current system* dapat dilihat pada Gambar 3.1 berikut.



Gambar 3.1. Current System Search Daftar Voting

Pada proses *search data polling* dilakukan oleh voter dan admin namun kedua pengguna ini memiliki perbedaan. Admin dan voter terlebih dahulu melakukan login untuk masuk ke dalam sistem. Setelah itu masuk ke halaman awal sistem. Pada halaman ini admin dan voter memilih menu survey lalu memilih polling. Setelah memilih menu polling voter dapat melihat daftar polling yang pernah dilakukan selain itu voter juga dapat melakukan search data voting dengan menggunakan *keyword* berdasarkan judul dan pertanyaan, selanjutnya voter

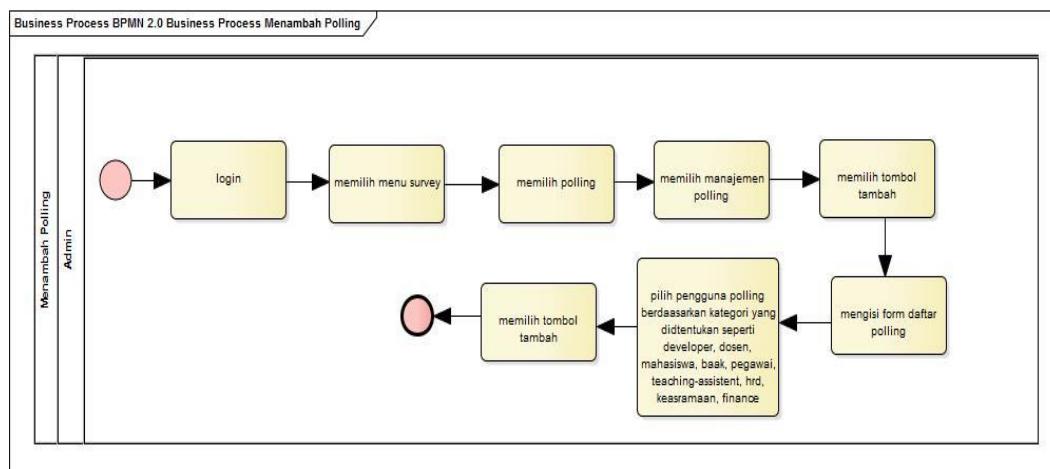
menekan tombol enter untuk pencarian data polling yang dituju. Setelah menekan tombol enter, voter dapat melihat hasil pencarian data voting yang dituju. Sedangkan pada admin setelah memilih menu polling maka admin dapat melihat daftar polling yang pernah dilakukan. Sebelum melakukan pencarian data polling, admin dapat memilih kategori polling berdasarkan semua polling yang terbaru atau berdasarkan history polling. Setelah memilih diantara keduanya admin dapat melihat *list* polling berdasarkan daftar polling yang telah dipilih, selanjutnya admin dapat melakukan search data voting dengan menggunakan keyword berdasarkan judul dan pertanyaan, kemudian menekan tombol enter untuk pencarian data polling yang dituju. Setelah menekan tombol enter, admin dapat melihat hasil pencarian data voting yang dituju.

2. Mengelola Daftar Polling

Berikut merupakan bisnis proses dari mengelola daftar polling.

1. Bisnis Proses Memasukkan Polling

Bisnis proses oleh admin untuk memasukkan polling pada current system dapat dilihat pada Gambar 3.2 berikut.

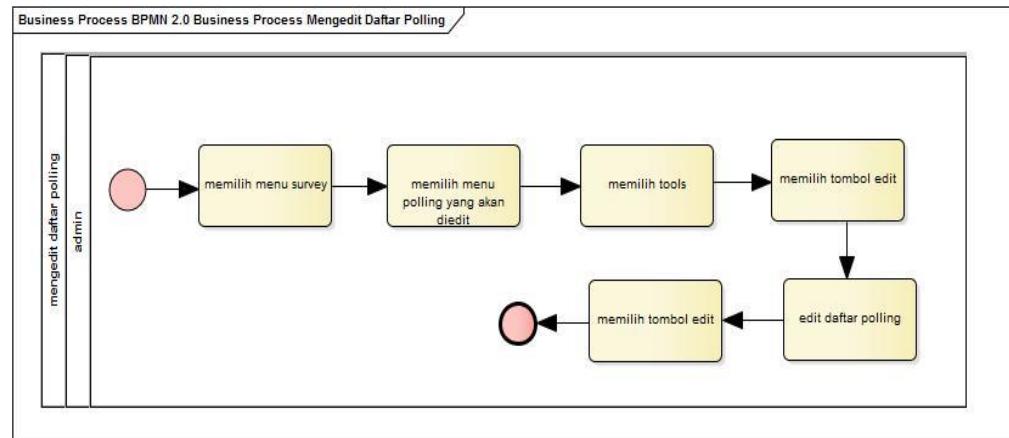


Gambar 3.2. Current System Memasukkan polling

Pada proses memasukkan polling dimulai dengan admin login terlebih dahulu selanjutnya memilih menu survey, memilih polling, memilih manajemen polling, memilih tombol tambah, mengisi daftar polling, selanjutnya pilih pengguna berdasarkan kategori yang telah ditentukan seperti developer, dosen, mahasiswa, baak, pegawai, teaching-assistant, hrd, keasramaan, dan finance dan pilih tombol tambah untuk menambahkan polling pada sistem.

2. Bisnis Proses Mengedit Daftar Polling

Bisnis proses oleh voter untuk mengedit daftar polling pada current system dapat dilihat pada Gambar 3.3 berikut.

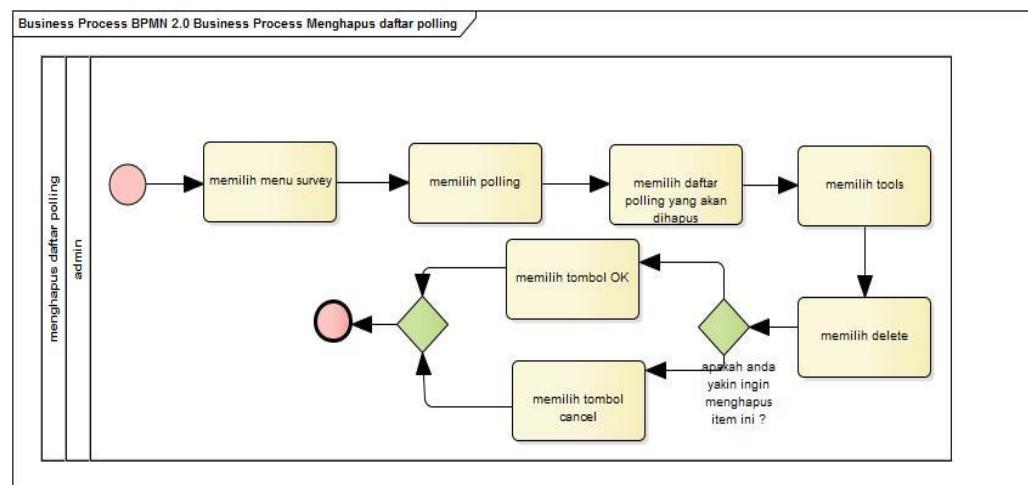


Gambar 3.3. Current System Mengedit Daftar polling

Pada proses mengedit daftar polling dimulai dengan admin login terlebih dahulu selanjutnya memilih menu survey, memilih polling yang akan diedit, memilih tools, memilih tombol edit, mengedit daftar polling pilih tombol edit untuk mengubah daftar polling pada sistem.

3. Bisnis Proses Menghapus Daftar Polling

Bisnis proses oleh voter untuk menghapus daftar polling pada current system dapat dilihat pada Gambar 3.4 berikut.



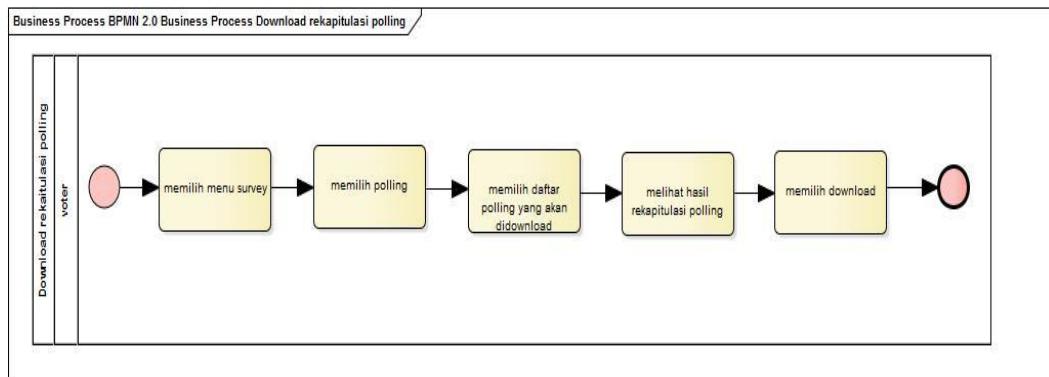
Gambar 3.4. Menghapus Daftar Polling

Pada proses menghapus daftar polling dimulai dengan admin login terlebih dahulu selanjutnya memilih menu survey, memilih polling, memilih polling yang akan dihapus, memilih tools, memilih delete, jika ingin menghapus item

polling pilih tombol OK dan jika tidak ingin menghapus item pilih tombol cancel.

3. Download Rekapitulasi Polling

Bisnis proses oleh voter untuk download rekapitulasi polling pada *current system* dapat dilihat pada Gambar 3.5 berikut.

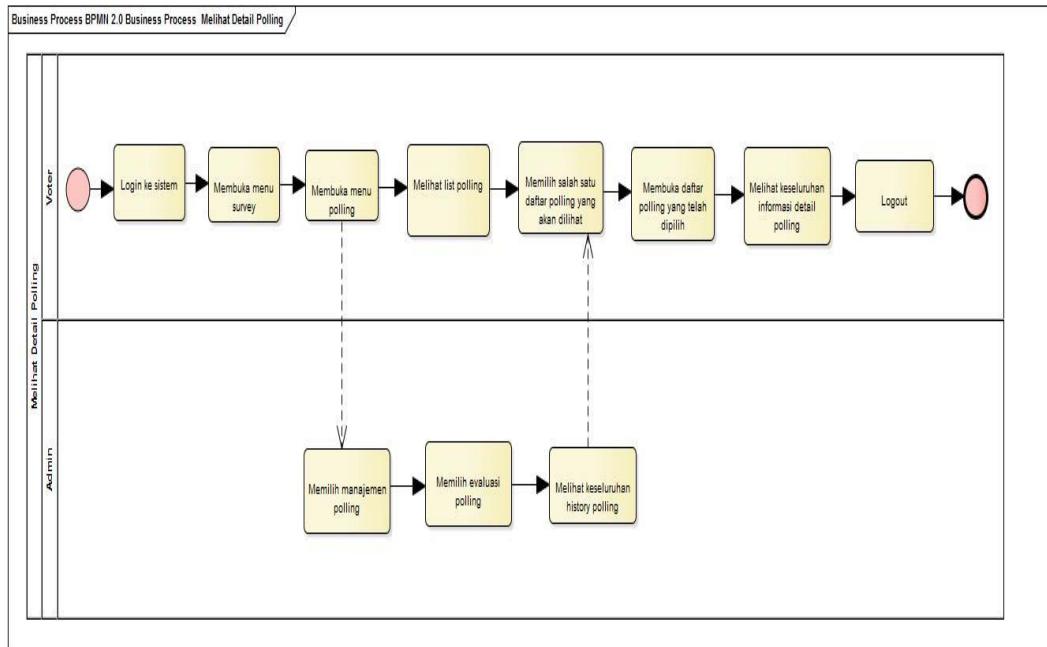


Gambar 3.5. Current System Download Rekapitulasi Polling

Pada proses download dimulai dengan login terlebih dahulu untuk masuk ke dalam sistem, lalu pilih menu survey kemudian pilih polling. Selanjutnya voter dapat melihat daftar polling, lalu memilih daftar polling yang akan didownload. Kemudian voter dapat melihat hasil rekapitulasi polling seperti nama kandidat, hasil vote setiap kandidat, dan jumlah voter. Selanjutnya pilih download hasil rekapitulasi polling dalam berbagai ekstensi file seperti image PNG, JPEG, PDF dokumen, dan SVG vector image. Apabila ingin keluar dari sistem pilih tombol *logout*.

4. Melihat Hasil Polling

Bisnis proses oleh voter dan admin untuk melihat hasil polling pada *current system* dapat dilihat pada Gambar 3.6 berikut.



Gambar 3.6. Current System Melihat Detail Polling

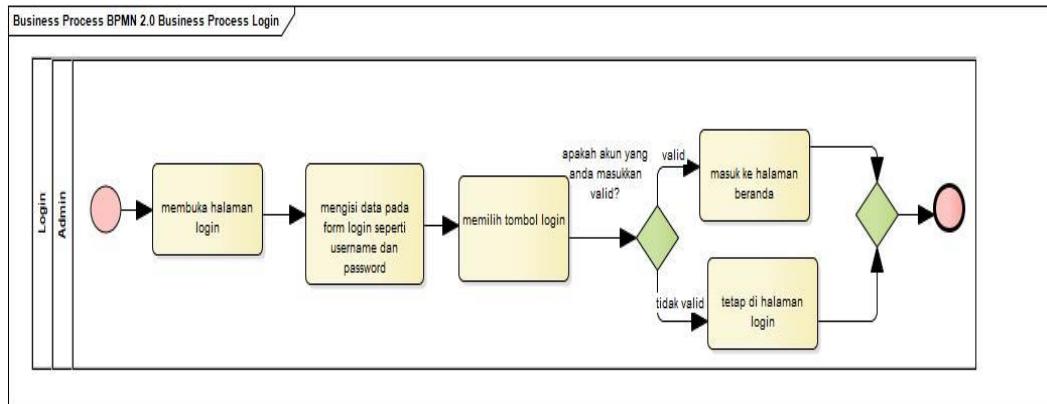
Pada proses melihat detail polling dimulai dengan voter dan admin terlebih dahulu login untuk masuk ke dalam sistem. Kemudian memilih menu survey lalu memilih polling. Selanjutnya voter dapat melihat list polling, sedangkan admin setelah memilih menu polling selanjutnya memilih manajemen polling kemudian memilih evaluasi polling. Setelah itu admin dapat melihat keseluruhan history polling yang pernah dilakukan. Selanjutnya admin dan voter dapat memilih salah satu daftar polling yang akan dilihat kemudian membuka daftar polling yang telah dipilih. Setelah itu admin dan voter dapat melihat keseluruhan informasi detail polling seperti informasi detail kandidat. Selanjutnya jika admin dan voter ingin keluar dari sistem pilih *logout*.

3.7 Target System System

Pada subbab ini akan dijelaskan target sistem yang akan dibangun.

1. Login

Bisnis proses oleh admin untuk *login* pada target system dapat dilihat pada Gambar 3.7 berikut.



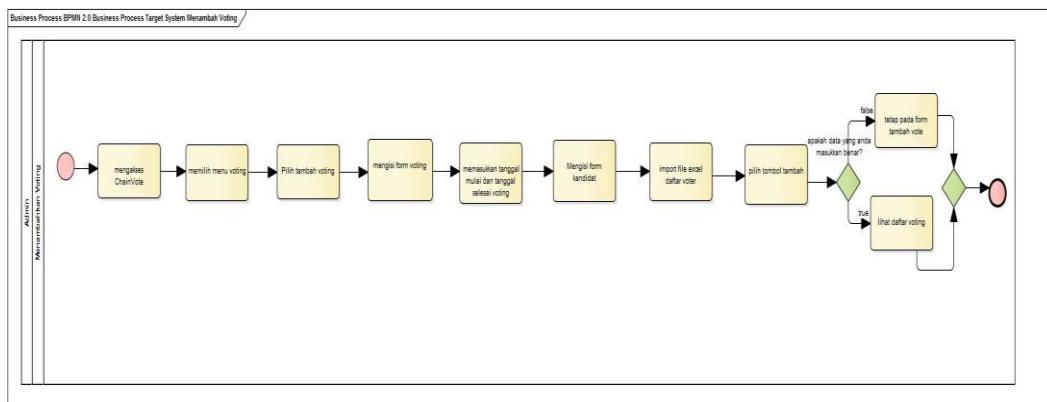
Gambar 3.7. Login

Keterangan :

Pada proses login oleh admin dimulai dengan membuka halaman login terlebih dahulu selanjutnya mengisi data pada form login yaitu username dan password lalu memilih tombol login. Apabila akun yang dimasukkan valid maka admin dapat masuk ke halaman beranda sedangkan jika akun yang dimasukkan tidak valid maka form akan menampilkan pesan error sehingga admin tetap di halaman login.

2. Menambahkan Voting

Bisnis proses oleh admin untuk menambahkan voting pada target system dapat dilihat pada Gambar 3.8 berikut.



Gambar 3.8. Target System Menambahkan Voting

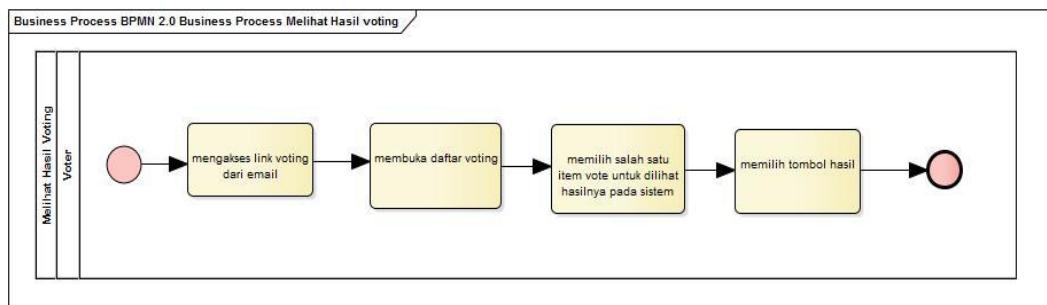
Keterangan :

Pada proses menambahkan voting dimulai dengan admin terlebih dahulu mengakses sistem ChainVote setelah itu memilih menu voting. Selanjutnya admin memilih menu tambah voting lalu mengisi form voting selanjutnya memasukkan waktu mulai dan selesai voting, mengisi form kandidat, kemudian mengimport

file excel daftar voter dan pilih tombol tambah untuk menyimpan dan menampilkan daftar voting yang telah didaftarkan. Jika data voting yang ditambahkan valid maka sistem akan menampilkan daftar voting namun jika data voting yang ditambahkan tidak valid maka sistem akan menampilkan pesan *error* dan admin tetap berada pada halaman tambah vote.

3. Melihat Hasil Voting

Bisnis proses oleh voter untuk melihat hasil voting pada target system dapat dilihat pada Gambar 3.9 berikut.



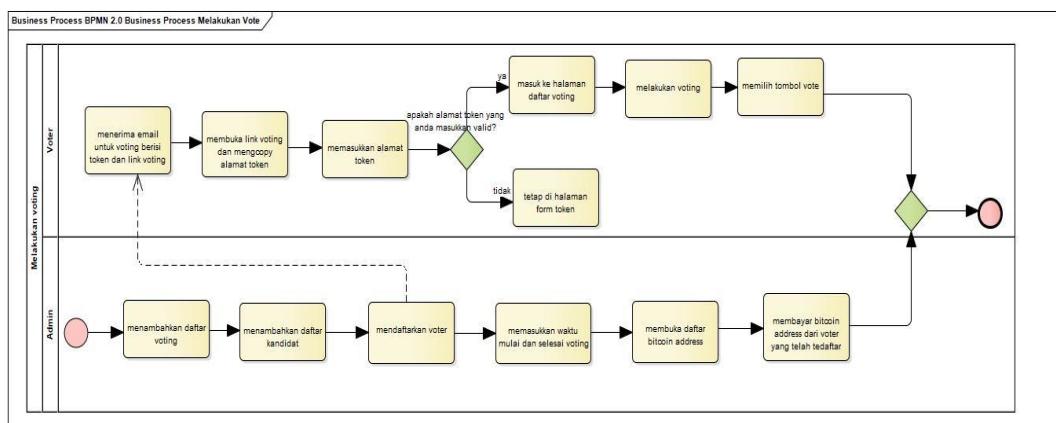
Gambar 3.9. Target System Melihat Hasil Voting

Keterangan :

Pada proses melihat hasil voting dimulai dengan voter yang telah melakukan voting mengakses link voting dari email selanjutnya membuka daftar voting. Setelah halaman daftar voting ditampilkan sistem voter memilih salah satu item vote untuk dilihat hasilnya pada sistem selanjutnya memilih tombol hasil untuk melihat hasil voting.

4. Melakukan Voting

Bisnis proses oleh voter untuk melakukan voting pada target system dapat dilihat pada Gambar 3.10 berikut.



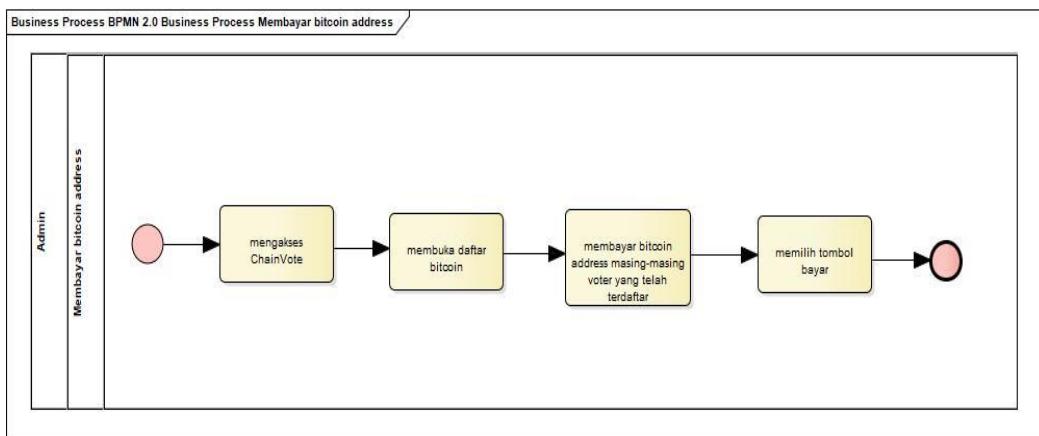
Gambar 3.10. Melakukan Voting

Keterangan :

Pada proses melakukan voting dimulai dengan admin akan terlebih dahulu menambahkan daftar voting, menambahkan daftar kandidat, mendaftarkan voter, memasukkan waktu mulai dan selesai voting, dan membayar bitcoin address dari voter yang telah terdaftar. Apabila admin telah mendaftarkan voter, voter akan menerima email untuk voting berisi alamat token dan link voting. Setelah itu voter akan membuka link voting. Setelah link untuk voting terbuka voter akan memasukkan alamat token pada halaman form token. Jika alamat token yang dimasukkan valid, voter akan masuk ke halaman vote untuk melakukan voting. Namun, jika alamat token yang dimasukkan tidak valid maka sistem akan menampilkan pesan *error* dan voter tetap berada pada halaman form memasukkan token.

5. Membayar Bitcoin Address

Bisnis proses oleh admin untuk membayar bitcoin address pada target system dapat dilihat pada Gambar 3.11 berikut.



Gambar 3.11. Membayar Bitcoin Address

Keterangan :

Pada proses membayar bitcoin address dimulai dengan admin akan mengakses Chain Vote lalu membuka daftar bitcoin. Setelah itu admin akan membayar bitcoin address dari masing-masing voter yang telah terdaftar dengan memilih tombol bayar. Setelah admin membayar bitcoin address maka status bitcoin address dari masing-masing voter akan berubah menjadi sudah dibayar.

3.7.1 User Characteristics

Berikut adalah karakteristik pengguna aplikasi Sistem E-Voting menggunakan Teknologi Blockchain berbasis web.

1. User Group 1

<i>Description of User</i>	: Admin
<i>Role</i>	: Admin dapat menambahkan voting, membuat daftar kandidat, mendaftarkan voter, memasukkan waktu mulai dan selesai voting, dan membayar bitcoin address dari daftar voter yang telah terdaftar.
<i>Prerequisite</i>	: Admin harus <i>login</i> terlebih dahulu untuk masuk ke dalam sistem.
<i>Task description</i>	: Menambahkan daftar voting meliputi membuat daftar kandidat, mendaftarkan voter, memasukkan waktu mulai dan selesai voting, dan membayar bitcoin address dari daftar voter yang telah terdaftar.

2. User Group 2

<i>Description of User</i>	: Voter
<i>Role</i>	: Voter dapat melakukan voting dan melihat hasil voting
<i>Prerequisite</i>	: Voter harus terdaftar pada sistem ChainVote dan memiliki token
<i>Task description</i>	: Melakukan voting dan melihat hasil voting

Voter pada sistem ini terdiri dari user yang terdaftar pada sistem ChainVote dan memiliki token untuk melakukan voting.

3.8 Analisis Environment

Pada subbab ini berisi penjelasan mengenai lingkungan perangkat lunak dan perangkat keras yang digunakan oleh tim developer dalam pembangunan dan pengoperasian Sistem E-voting menggunakan Teknologi Blockchain yang mencakup lingkungan pengembangan dan lingkungan operasional.

3.8.1 Operational Environment

Operational environment menjelaskan mengenai spesifikasi aplikasi yang dibutuhkan dalam pengoperasian Sistem E-voting menggunakan Teknologi Blockchain. Semua kebutuhan ini berguna agar sistem dapat berjalan atau beroperasi dengan baik. Untuk pengoperasian sistem ini dibutuhkan piranti sebagai berikut :

1. Spesifikasi *software* lingkungan operasional aplikasi antara lain :
 1. *Operating System* : Windows 10
 2. Paket *office* : Microsoft Office 2016
 3. *Development Tools* : PHP Storm, SQLYog
 4. *Browser* : Google Chrome dan Mozilla
 5. *Programming Language* : PHP dan JavaScript
 6. *Design Tools* : Enterprise Architect, Balsamiq Mockups 3, dan Power Designer 15.2
 7. *Framework* : Yii2
 8. *Library* : Bitcoin PHP dan Bitcoin JS
 9. *Database* : MySQL
 10. Tesnet Bitcoin : API / SoChain
2. Spesifikasi *hardware* lingkungan operasional aplikasi antara lain :
 1. *Processor* : Intel ® Core(TM) i5-3230M CPU @2.60GHz (4 CPUs), 2.6GHz
 2. *RAM* : 8GB

3.9 Lingkungan Pengujian

Pada bagian ini dijelaskan mengenai lingkungan yang dibutuhkan dalam pengujian sistem, rencana dan pengendalian sumber daya (perangkat lunak dan perangkat keras) yang akan melakukan pengujian.

3.9.1 Perangkat Lunak Pengujian

Spesifikasi minimal *software* yang harus dipersiapkan untuk melakukan pengujian yang digunakan oleh tim *developer* adalah :

1. Operating System : Windows 10

2. Development Tools : PHP Storm
3. Browser : Google Chrome
4. Framework : Yii2, SoChain
5. Library : Bitcoin PHP dan Bitcoin JS

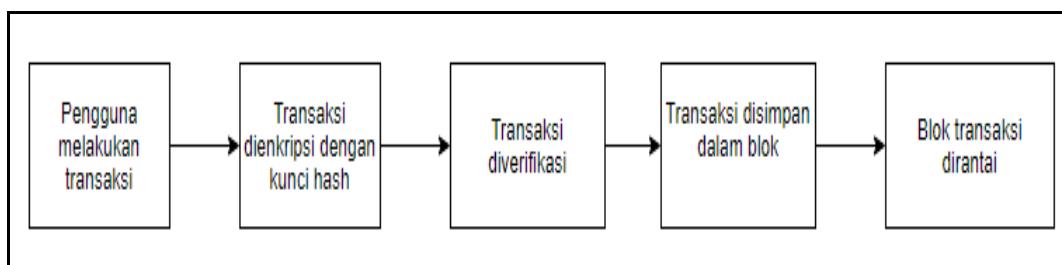
3.9.2 Perangkat Keras Pengujian

Spesifikasi minimal *hardware* yang harus dipersiapkan untuk melakukan pengujian yang digunakan oleh tim *developer* adalah :

1. Laptop : Lenovo
2. Processor : Intel® Core™ i5-3230M CPU @ 2.60GHz
3. RAM : 12.00 GB
4. Hard Disk : 500 GB

3.10 Analisis Teknologi Blockchain

Pada subbab berikut akan dijelaskan mengenai proses kerja transaksi yang ada di bitcoin yaitu pengiriman mata uang bitcoin dalam teknologi blockchain dapat dilihat pada Gambar 3.12 berikut :



Gambar 3.12. Proses Kerja transaksi dalam Teknologi Blockchain

Skema ini merupakan mekanisme transaksi pengiriman mata uang digital dalam teknologi blockchain. Pada skema ini proses yang terjadi yaitu pengguna saling melakukan transaksi dengan pengguna lain. Pengguna yang terlibat dalam transaksi ini tidak saling mengenal tetapi setiap salinan transaksi tereplikasi di semua komponen pengguna. Transaksi yang telah dilakukan pengguna di hash dengan cara mengenkripsi data transaksi tersebut, setelah itu data transaksi akan diverifikasi dimana hasil verifikasi akan disimpan dalam blok yang baru. Hasil dari mekanisme yaitu semua blok transaksi yang baru dirantai dalam rangkaian

blok secara permanen. Adapun penjelasan dari mekanisme transaksi dalam blockchain adalah sebagai berikut :

1. Pengguna saling melakukan transaksi

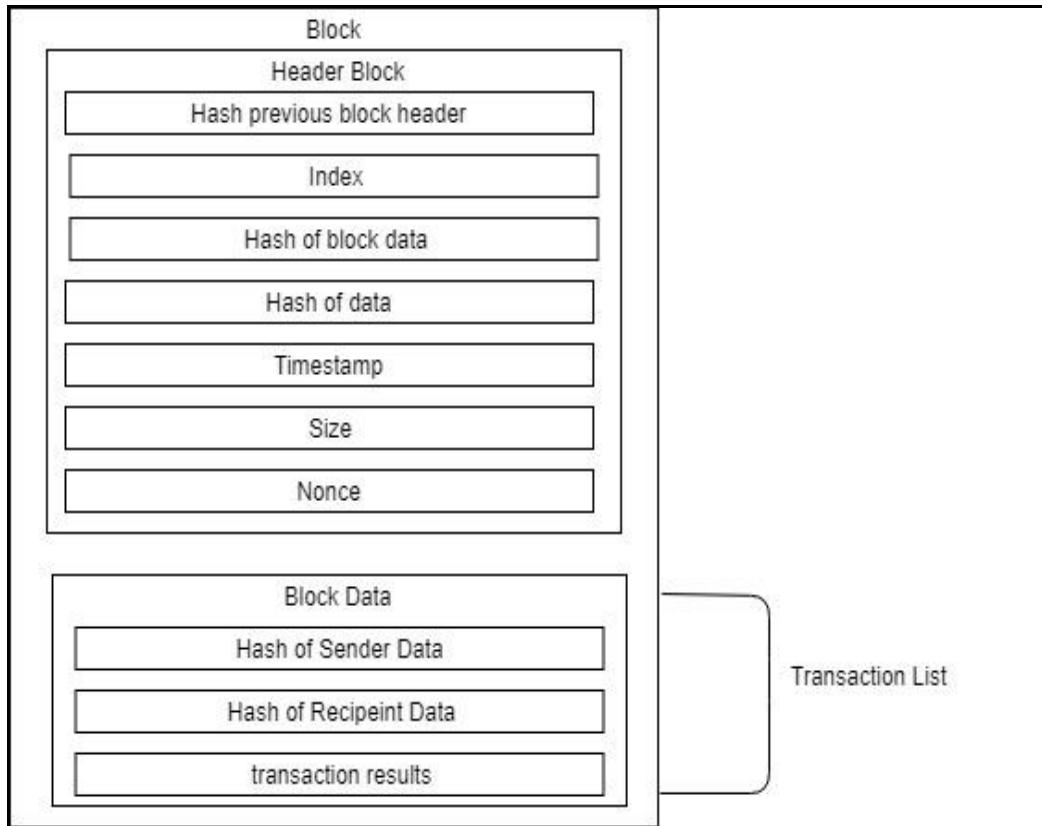
Pada jaringan blockchain, pengguna saling melakukan transaksi. Pengguna pada jaringan blockchain mengirimkan transaksi ke jaringan blockchain melalui perangkat lunak seperti aplikasi desktop, smartphone, dompet digital, layanan web, dan lain-lain. Perangkat lunak ini mengirimkan transaksi ke node yang satu dengan node yang lain dalam jaringan blockchain. Transaksi yang sudah diajukan disebarluaskan ke node lain di jaringan sampai transaksi akan diverifikasi. Proses pendistribusian transaksi ini ke node lain sampai membentuk jaringan *peer to peer* yang mencakup semua node pada sistem ini. Setiap komponen pada sistem ini harus terkoneksi terlebih dahulu satu sama lain, dan juga terhubung dengan *control* node.

2. Transaksi dienkripsi menggunakan kunci hash

Setiap transaksi yang dilakukan pengguna dihash dengan mengenkripsi data transaksi. Tujuan pembuatan hash pada data untuk memastikan bahwa tidak ada yang mengetahui isi data yang telah dibuat.

Blok transaksi berisi header blok dan data blok. Block header berisi kumpulan-kumpulan transaksi untuk blok ini seperti nomor blok, nilai hash blok sebelumnya, *timestamp*, ukuran blok, dan nilai *nonce*. Data blok berisi daftar transaksi yang divalidasi dan otentik yang telah dikirimkan ke blockchain.

Berikut struktur block dalam blockchain seperti pada Gambar 3.13 berikut ini.



Gambar 3.13. Struktur Block dalam Blockchain

Keterangan :

Struktur data blockchain umumnya terdiri dari :

1. *Block Header*

1. Nomor blok : Nomor indeks dari setiap blok untuk memudahkan pengurutan blok dan proses pengelompokan blok yang valid.
2. Hash blok sebelumnya : Digunakan untuk memastikan tidak ada data di dalam blockchain sebelum block ini berubah.
3. Data hash : Hash dari keseluruhan data transaksi untuk memastikan tidak ada data yang berubah
4. Block hash : Hash dari keseluruhan block
5. Timestamp : Penanda waktu untuk penyelesaian blok dari proses mining
6. Nilai nonce : Angka acak untuk proses mining dalam menemukan hash yang cocok untuk block selanjutnya.
7. Size : Ukuran transaksi dalam satuan per *byte*.

2. *Block Data*

1. Daftar transaksi dalam blok berisi data pengirim, data penerima, dan jumlah transaksi yang telah dienkripsi dalam bentuk hash agar identitas pengirim, penerima, dan jumlah transaksinya tetap tidak diketahui.
2. Data lain yang mungkin ada seperti nomor index kandidat pilihan dan penanda waktu pemilihan.

3. Transaksi diverifikasi

Setiap transaksi mata uang digital akan diverifikasi untuk dilakukan pengecekan, apabila transaksi tersebut valid maka informasi mengenai transaksi akan disimpan pada blok baru. Keaslian suatu pesan dijamin dengan memeriksa bahwa transaksi tersebut diformat dengan benar. Node sebelumnya akan memeriksa validitas dan keaslian transaksi dalam blok yang dipublikasikan dan tidak akan menyimpan blok jika berisi transaksi yang tidak valid.

Tahapan untuk melakukan proses verifikasi pada transaksi :

1. Pengguna memasukkan identitas sesuai informasi pada halaman login.
2. Pengguna melakukan transaksi dengan pengguna lainnya.
3. Hasil transaksi akan dienkripsi menggunakan kunci private pengguna.
4. Setelah transaksi diamankan dengan menggunakan kunci hash, hasil hash tersebut dikirimkan ke control node untuk memverifikasi informasi yang disediakan.
5. Jika hasil transaksi tersebut valid maka sistem akan menyimpan informasi pengguna termasuk id pengguna, email, dan hasil transaksi.
4. Transaksi disimpan dalam Blok

Proses mining dilakukan untuk memverifikasi dan menemukan hash yang tepat dari sebuah blok agar dapat ditambahkan ke dalam blok baru. Proses mining merupakan sebuah kegiatan menambang menggunakan perangkat tertentu atau disebut sebagai miner. Para penambang (miner) akan

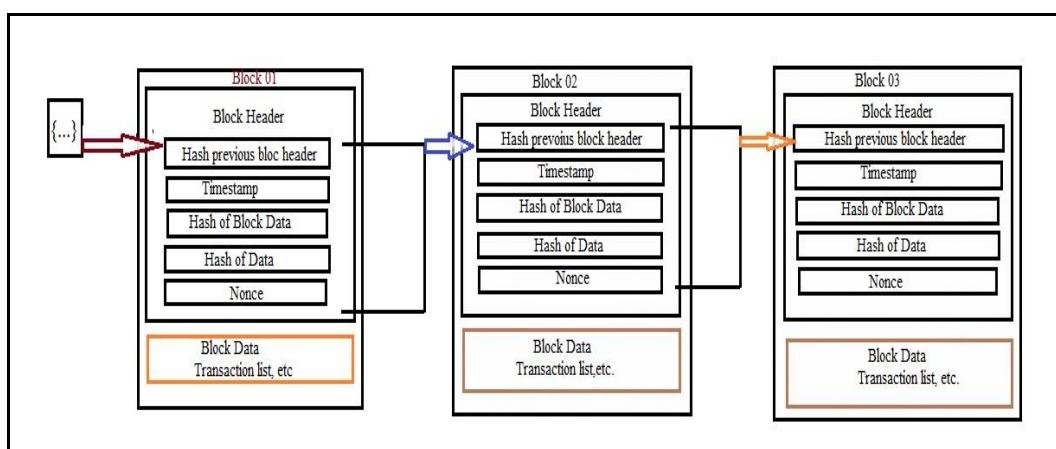
memvalidasi setiap transaksi, membangun, dan menyimpan blok dari tersebut ke dalam blockchain. Proses mining yang dilakukan dalam sistem ini adalah sebagai berikut :

1. Data transaksi yang sudah valid dikumpulkan bersama dengan data transaksi lainnya.
2. Data transaksi tersebut kemudian disimpan ke dalam sebuah blok, selanjutnya para penambang (miner) mulai melakukan proses mining terhadap blok tersebut.
3. Blok tersebut kemudian dikirimkan ke node yang saling terhubung untuk diverifikasi dan disimpan dalam blok baru dalam blockchain.

Proses mining ini bertujuan untuk menghindari data transaksi yang random dalam blockchain dan untuk memudahkan pengelompokan data transaksi yang valid untuk mendeteksi dan menolak blok yang tidak valid.

5. Blok transaksi Dirantai

Setiap blok yang berisi hash dari header blok sebelumnya dirantai secara bersama-sama sehingga membentuk blockchain. Jika blok yang sebelumnya diubah dengan memiliki hash yang berbeda dapat menyebabkan semua blok berikutnya juga memiliki hash yang berbeda karena menyertakan hash dari blok sebelumnya. Ini memungkinkan dengan mudah untuk mendeteksi dan menolak blok yang diubah. Jadi transaksi dianggap selesai apabila hasil transaksi telah ditambahkan pada blok yang baru dan dienkripsi secara permanen dalam rantai blok. Berikut Gambar 3.14 menunjukkan rangkaian rantai blok dalam blockchain.



Gambar 3.14. Rangkaian rantai block dalam blockchain

3.11 Analisis Sistem E-Voting Menggunakan Teknologi Blockchain

Teknologi yang dimanfaatkan untuk pembangunan sistem e-voting kegiatan pemilihan mahasiswa di IT Del yaitu menggunakan teknologi blockchain. Setiap transaksi voting pada blockchain dicatat pada blok-blok. Jadi setiap blok berisi transaksi yang terjadi pada waktu tertentu. Nilai hash dari blok saat ini dan nilai hash dari blok sebelumnya akan menjadi input dari nilai hash blok berikutnya. Jadi setiap blok saling berhubungan dengan blok berikutnya. Berikut Gambar 3.15 menunjukkan struktur penyimpanan data voting di blockchain.



Gambar 3.15. Struktur penyimpanan transaksi voting di blockchain

Keterangan :

Pada Gambar 26 menunjukkan blockchain sebagai basis data penyimpanan transaksi voting. Berikut deskripsi struktur blok penyimpanan transaksi voting pada blockchain :

1. **ID Transaksi (Transaction ID / TXID)**

ID Transaksi adalah ID sebuah transaksi. Setiap ID Transaksi memiliki ID yang berbeda-beda. Fungsi ID Transaksi adalah untuk mencari detail informasi atas segala sesuatu yang berelasi dengan transaksi tersebut. Dengan ID Transaksi ini kita dapat mengetahui apakah transaksi tersebut telah dibroadcast dan dikonfirmasi oleh para penambang. Suatu transaksi benar-benar dilakukan apabila transaksi tersebut telah disiarkan ke jaringan blockchain.

2. **Block Hash**

Block Hash merupakan hash dari keseluruhan blok.

3. **Address Pengirim**

Address pengirim adalah identitas pengirim transaksi. Identitas pengirim digantikan dengan deret angka dan huruf sebenarnya adalah *hash public key*.

4. **Output Script**

Output script menjelaskan tentang script output dan berelasi dengan address penerima dalam transaksi tersebut.

5. **Input Script**

Input script menjelaskan tentang detail script yang berasal dari output transaksi sebelumnya. Jadi jika output transaksi sebelumnya berelasi dengan banyak transaksi, maka akan tertulis detail input yang digunakan pada transaksi tersebut.

6. **Address Penerima**

Address penerima adalah *address* penerima transaksi.

7. **Spent/Unspent**

Spent dan *unspent* untuk menunjukkan apakah sejumlah bitcoin yang diterima oleh pemilik *address* tersebut telah digunakan untuk transaksi atau belum. Jika transaksi tersebut telah digunakan maka statusnya adalah “spent”, namun jika transaksi tersebut belum digunakan atau ditransaksikan maka statusnya adalah “unspend”.

8. **Confirmations/Konfirmasi**

Konfirmasi menunjukkan status transaksi apakah telah diproses oleh para penambang atau belum. Transaksi yang telah masuk ke dalam *block* yang

valid jika transaksi tersebut telah mendapat minimal 6 konfirmasi. Pada umumnya jumlah konfirmasi akan terus bertambah. Blok–blok baru bitcoin akan diproduksi dalam rentang waktu 10 menit maka pertambahan jumlah konfirmasi juga akan terus bertambah. Jadi transaksi yang mendapat jumlah konfirmasi semakin banyak maka validitasnya juga akan semakin meningkat. Sehingga blok pada transaksi semakin sulit untuk dimanipulasi.

9. Total nilai transaksi

Total nilai transaksi adalah penjelasan mengenai total nilai transaksi dalam satuan BTC.

10. Ukuran transaksi

Ukuran transaksi menjelaskan tentang ukuran transaksi dalam satuan per byte. Semakin besar ukuran transaksi maka semakin besar pula biaya transaksi yang dikenakan.

11. Time

Time menunjukkan penanda waktu kapan transaksi tersebut diterima dan dinyatakan valid sampai transaksi – transaksi yang terjadi dimasukkan ke dalam blok baru yang valid.

12. Included in block

Menunjukkan di blok manakah transaksi tersebut dimasukkan. Pada bitcoin transaksi dimasukkan ke dalam blok–blok baru dimana setiap blok tersebut mempunyai ID tersendiri. Di setiap blok terdapat blok header yang berguna untuk memberikan informasi singkat isi dalam blok dan transaksi apa yang terjadi di dalamnya.

13. Fee

Fee merupakan biaya transaksi yang digunakan untuk memproses transaksi. Karena semakin besar ukuran transaksi maka memprosesnya membutuhkan lebih banyak waktu dan energi (listrik).

Dalam implementasi sistem akan mengambil detail *output script* pada penyimpanan data blockchain sebagai pesan kode transaksi voting. Struktur *output script* menyimpan detail transaksi voting *message* kode OP_RETURN hasil vote dalam format *hexadecimal*. OP_RETURN adalah sebuah tumpukan skrip tanpa perulangan. Dalam *protocol* bitcoin, OP_RETURN dapat menyimpan

sampai 80 byte dalam transaksi. Untuk mengkonversi atau mendekode kode OP_RETURN (*hexadecimal*) menjadi bentuk karakter, peneliti menggunakan *hex2bin()* sehingga mudah dibaca oleh penerima pesan.

Oleh karena itu peneliti akan menggunakan salah satu API untuk mempercepat proses *development* sistem e-voting. Salah satu API Blockchain yang akan digunakan peneliti adalah API SoChain. API SoChain adalah layanan yang digunakan untuk membuat dan mengambil transaksi voting di testnet bitcoin berdasarkan bitcoin address. Bitcoin address *digenerate* menggunakan *library* Bitcoin PHP. Layanan ini yang akan digunakan untuk membuat dan mengambil kode OP_RETURN pada *outputs script* di penyimpanan data blockchain. Transaksi voting diambil dan ditandatangani dalam format hex dan mengirimkannya ke jaringan blockchain menggunakan metode POST. Representasi hex dari transaksi berupa objek JSON.

Selanjutnya transaksi voting ini akan diverifikasi untuk mengetahui bahwa hasil voting dihitung dengan benar. Untuk detailnya penulis menampilkan struktur detail transaksi voting yang telah dihubungkan pada API SoChain menggunakan software pengujian bitcoin tesnet pada Gambar 3.16 berikut :

```
"outputs" : [
    {
        "output_no" : 0,
        "address" : "nulldata",
        "value" : "0.00000000",
        "type" : "nulldata",
        "req_sigs" : null,
        "spent" : null,
        "script_asm" : "OP_RETURN 766f74696e674b6d62303131",
        "script_hex" : "6a0c766f74696e674b6d62303131"
    },
]
```

Gambar 3.16. Struktur detail transaksi voting pada API SoChain

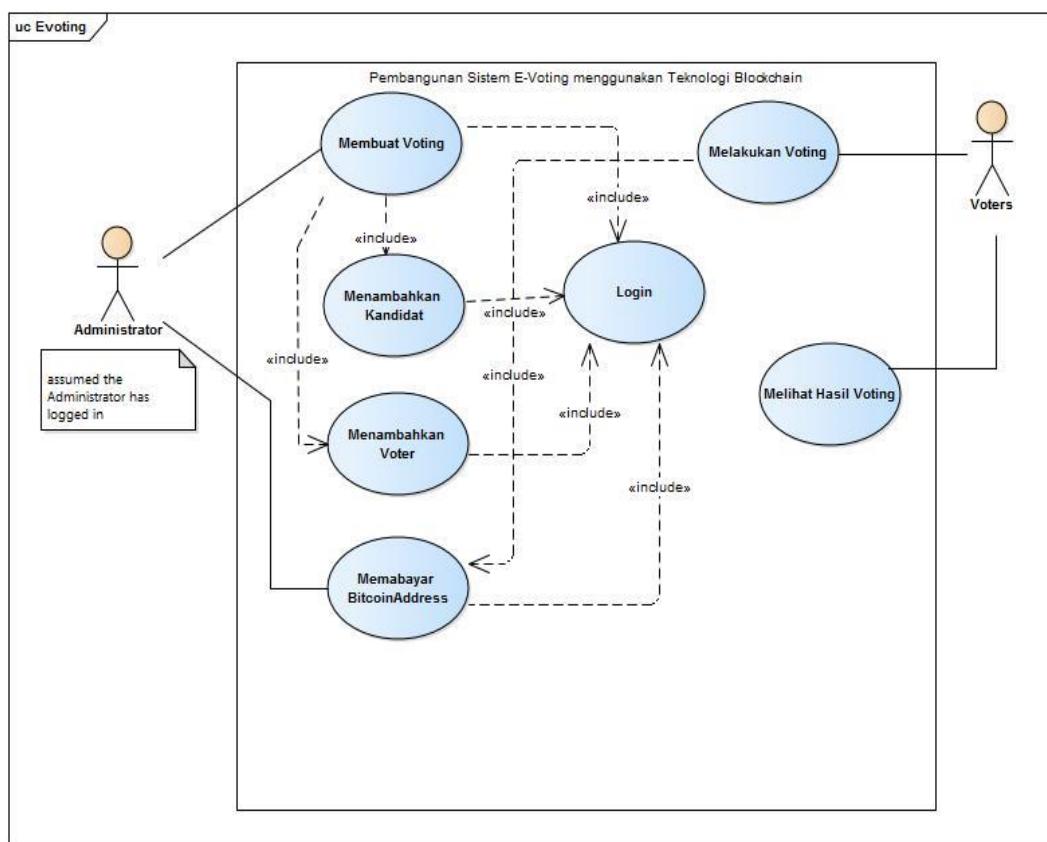
Keterangan :

Dari Gambar 26 struktur detail transaksi voting pada outputs script, kita dapat melihat bahwa *output-script* menunjukkan kode OP_RETURN 766f74696e674b6d62303131 sebagai hasil transaksi voting pada blockchain. layanan API SoChain digunakan untuk membuat dan mengambil transaksi voting. Dalam implementasi peneliti menggunakan OP_RETURN untuk menyimpan

pesan transaksi voting. Untuk mendekode OP_RETURN, kita dapat menggunakan fungsi `hex2bin()` untuk mengubahnya ke karakter. Dengan mendekode OP_RETURN kita bisa mendapatkan pesan /transaksi voting yaitu “voting011007”.

3.12 Use Case Diagram

Use case diagram menggambarkan hal apa saja yang dapat dilakukan oleh aktor terhadap suatu sistem. Berikut Gambar 3.17 *use case diagram* dari sistem yang akan dibangun.



Gambar 3.17. Use Case Diagram

Berdasarkan Gambar 3.17 *use case diagram* ada 2 aktor yang menggunakan sistem yaitu administrator dan voter. Administrator diasumsikan telah login ke dalam sistem untuk melakukan role yang telah ditentukan. Pada saat admin membuat voting admin juga menambahkan kandidat dan menambahkan voter. Admin juga dapat membayar bitcoin address. Sedangkan voter yang menggunakan sistem ini user yang telah terdaftar pada sistem dan memiliki token.

Voter dapat melakukan voting setelah admin membayar bitcoin address voter. Selanjutnya setelah melakukan voting voter dapat melihat hasil voting.

3.13 Use Case Scenario

Pada sub bab ini akan dijelaskan *use case scenario* dari setiap fungsi yang telah digambarkan pada *use case diagram*.

3.13.1 Use Case Scenario Login

Use case scenario login dapat dilihat pada tabel 3.1 berikut.

Tabel 3.1. Use Case Scenario Login

Use Case ID Number	UC-1	
Use Case Name	Login	
Brief Description	Use Case untuk login ke dalam sistem	
Actor	Admin	
Precondition	Admin telah memiliki akun	
	Actor	System Response
	1. memasukkan username dan password	
	2. Klik tombol login	
		3. Sistem melakukan validasi
		4. Sistem akan menampilkan halaman beranda
Alternate Flow of Event		
Post Condition	Admin dapat masuk ke halaman utama	

3.13.2 Use Case Scenario Membuat Voting

Use case scenario membuat daftar voting dapat dilihat pada tabel 3.2 berikut.

Tabel 3.2. Use Case Scenario Membuat Voting

Use Case ID Number	UC-2	
Use Case Name	Membuat Voting	
Brief Description	Use Case untuk membuat voting (<i>Include</i> Menambahkan kandidat dan Voter)	
Actor	Admin	
Precondition	Admin telah mengakses sistem ChainVoting	
	Actor	System Response
	1. Memilih menu	

	tambah voting	
		2. Menampilkan form Tambah Voting
	3. Mengisi form Voting seperti judul, deskripsi, tanggal mulai dan tanggal berakhir voting.	
	4. Menambahkan kandidat [Tabel 4]	
	5. Menambahkan Voter [Tabel 5]	
	6. Admin memilih tombol tambah	
		7. Menyimpan data Voting
		8. Menampilkan Rincian Voting
Alternate Flow of Event		
Post Condition	Admin berhasil membuat daftar voting	

3.13.3 Use Case Scenario Menambahkan Kandidat

Use case scenario menambah kandidat dapat dilihat pada tabel 3.3 berikut.

Tabel 3.3. Use Case Scenario Menambahkan Kandidat

Use Case ID Number	UC-3	
Use Case Name	Membuat Daftar Kandidat	
Brief Description	Use Case untuk Menambahkan kandidat	
Actor	Admin	
Precondition	Admin telah mengisi form Voting [Tabel 2]	
	Actor	System Response
	1. Menekan Tombol tambah kandidat sebanyak yang dibutuhkan	
		2. Menampilkan form kandidat sebanyak yang diklik
	3. Mengisi Form Kandidat seperti Nama dan Deskripsi	

Alternate Flow of Event	
Post Condition	Admin berhasil membuat daftar kandidat

3.13.4 Use Case Scenario Menambahkan Voter

Use case scenario menambahkan voter dapat dilihat pada tabel 3.4 berikut.

Tabel 3.4. Use Case Scenario Menambahkan Voter

Use Case ID Number	UC-4	
Use Case Name	Menambahkan Voter	
Brief Description	Use Case untuk Menambahkan voter	
Actor	Admin	
Precondition	Admin telah mengisi form Voting dan mengisi/menambahkan kandidat	
	Actor	System Response
	1. Menekan tombol download template excel untuk daftar voter	
	2. Mengirim file template	
	3. Mengisi daftar voter pada excel	
	4. Admin memilih <i>choose</i> file	
	5. Admin memasukkan file excel daftar pemilih	
	6. Sistem akan menyimpan daftar pemilih	
Alternate Flow of Event		
Post Condition	Admin berhasil menambahkan voter dengan import excel	

3.13.5 Use Case Scenario Membayar Bitcoin Address

Use case scenario membayar bitcoin address yang telah terdaftar dapat dilihat pada tabel 3.5 berikut.

Tabel 3.5. Use Case Scenario Membayar Bitcoin Address

Use Case ID Number	UC-6
Use Case Name	Membayar Bitcoin Address
Brief Description	Use Case untuk membayar bitcoin address yang akan

	digunakan voter untuk melakukan voting	
Actor	Admin	
Precondition	Admin memiliki Balance Bitcoin yang cukup	
	Actor	System Response
	1. Admin memilih menu daftar bitcoin	
	2. Sistem akan menampilkan daftar bitcoin	
	3. Admin memilih tombol Aktivasi	
	4. Sistem akan menampilkan status bitcoin address menjadi aktif	
Alternate Flow of Event		
Post Condition	Admin berhasil menghentikan voting	

3.13.6 Use Case Scenario Melakukan Voting

Use case scenario melakukan vote dapat dilihat pada tabel 3.6 berikut.

Tabel 3.6. Use Case Scenario Melakukan Vote

Use Case ID Number	UC-9	
Use Case Name	Melakukan Vote	
Brief Description	Use Case untuk melakukan vote	
Actor	Voter	
Precondition	Voter menerima email untuk melakukan voting dan sudah memiliki Token dan mengakses Link yang diberikan	
	Actor	System Response
	1. Voter membuka emailnya untuk melihat token dan link untuk melakukan voting	
	2. Membuka link voting dan mengcopy token	
		3. Menampilkan form untuk memasukkan token
	4. Memasukkan token pada form token	
		5. Memverifikasi token yang dimasukkan, jika alamat token yang dimasukkan

		valid maka voter dapat masuk ke halaman vote, namun jika alamat token yang dimasukkan voter tidak valid maka sistem akan menampilkan <i>message error</i> "Maaf, Token anda tidak valid" dan tidak akan masuk ke halaman voting
		6. Menampilkan daftar kandidat yang akan di vote
	7. Menekan tombol vote	
		8. Sistem akan menampilkan bahwa vote berhasil dilakukan dan menampilkan detail hasil voting serta status waktu voting
Alternate Flow of Event	Actor	System Response
	1. Mengakses daftar menu voting	
	2. Menampilkan daftar voting	
	3. Menekan tombol untuk masuk ke form token	
	4. Menampilkan form token	
	5. Memasukkan token	
	6. Memverifikasi token yang dimasukkan, jika alamat token yang dimasukkan valid maka voter dapat masuk ke halaman vote, namun jika alamat token yang dimasukkan voter tidak valid maka sistem akan menampilkan <i>message error</i> "Maaf,	

		Token anda tidak valid” dan tidak akan masuk ke halaman voting
		7. Menampilkan daftar kandidat yang akan di vote
	8. Menekan tombol vote	
		9. Sistem akan menampilkan bahwa vote berhasil dilakukan dan menampilkan detail hasil voting serta status waktu voting
Post Condition	Voter berhasil melakukan voting	

3.13.7 Use Case Scenario Melihat Hasil Voting

Use case scenario melihat hasil voting dapat dilihat pada tabel 3.7 berikut.

Tabel 3.7. Use Case Scenario Melihat Hasil Voting

Use Case ID Number	UC-7	
Use Case Name	Melihat Hasil Voting	
Brief Description	Use Case untuk melihat hasil voting	
Actor	Admin & Voter	
Precondition	Voter telah melakukan voting	
	Actor	System Response
	1. Mengakses Daftar Voting	
		2. Menampilkan Daftar Voting
	3. Memilih Voting	
		4. Menampilkan detail dari voting
	5. Admin memilih tombol hasil	
		6. Sistem akan menampilkan hasil voting
Alternate Flow of Event		
Post Condition	Voter berhasil melihat hasil voting	

BAB 4

DESAIN

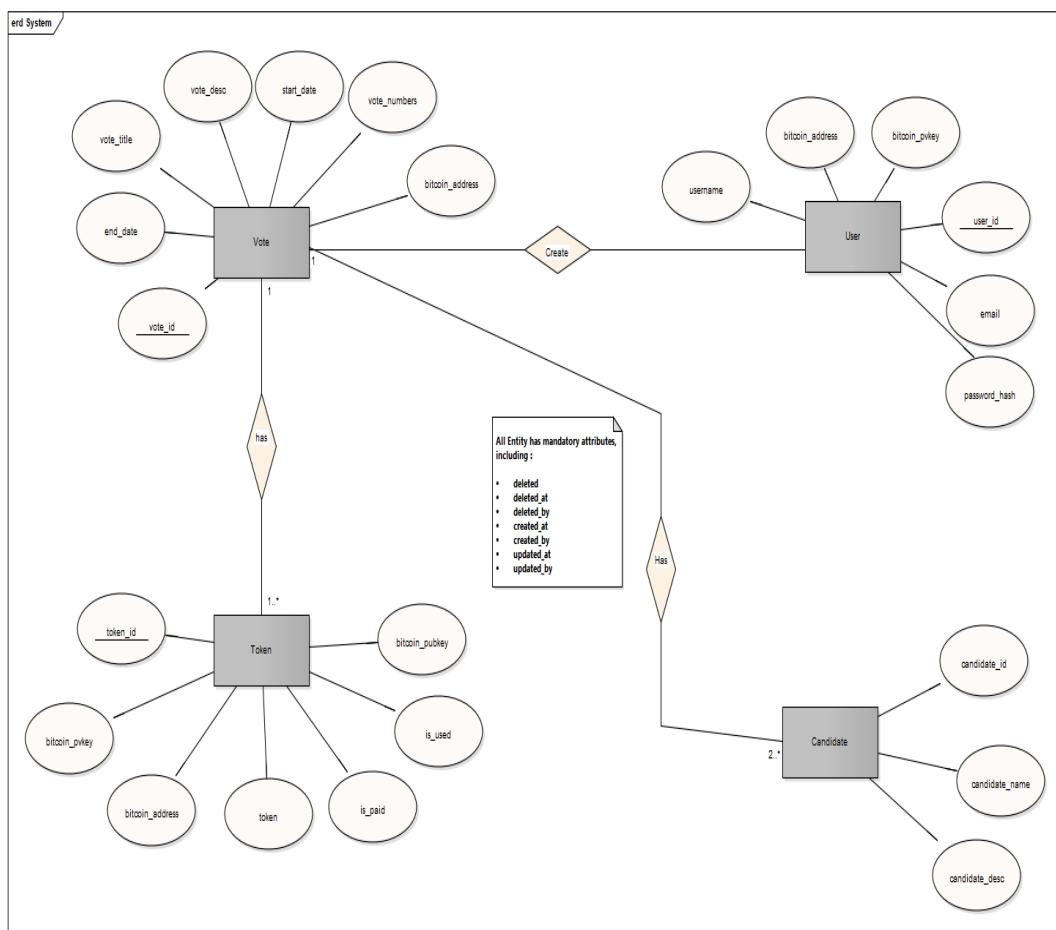
Pada bab ini dijelaskan mengenai desain aplikasi yang meliputi *data requirement*, *domain model*, *conceptual data*, *physical data*, *class diagram*, dan *sequence diagram* yang meliputi kebutuhan aplikasi dan batasan implementasi aplikasi sistem e-voting menggunakan teknologi blockchain.

4.1 Data Requirement

Pada subbab ini dijelaskan kebutuhan data selama pembangunan sistem e-voting menggunakan teknologi blockchain dalam bentuk ER-Diagram.

4.1.1 E-R Diagram

E-R Diagram yang digunakan dalam pembangunan Sistem E-voting menggunakan Teknologi Blockchain dapat dilihat pada Gambar 4.1 berikut.



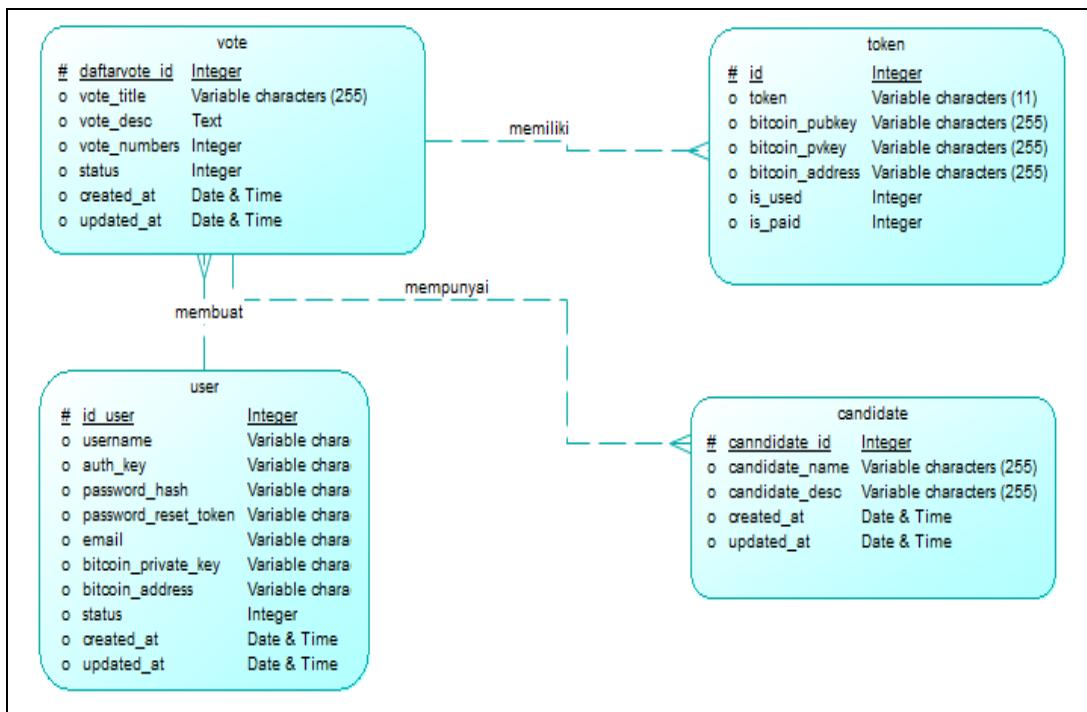
Gambar 4.1. E-R Diagram

4.2 Desain Sistem E-Voting menggunakan Blockchain

Pada bab ini dijelaskan diagram yang digunakan sebagai desain dari aplikasi yang dibangun yaitu *domain model*, CDM, PDM, *class diagram*, dan *sequence diagram*.

4.2.1 Conceptual Data Model (CDM)

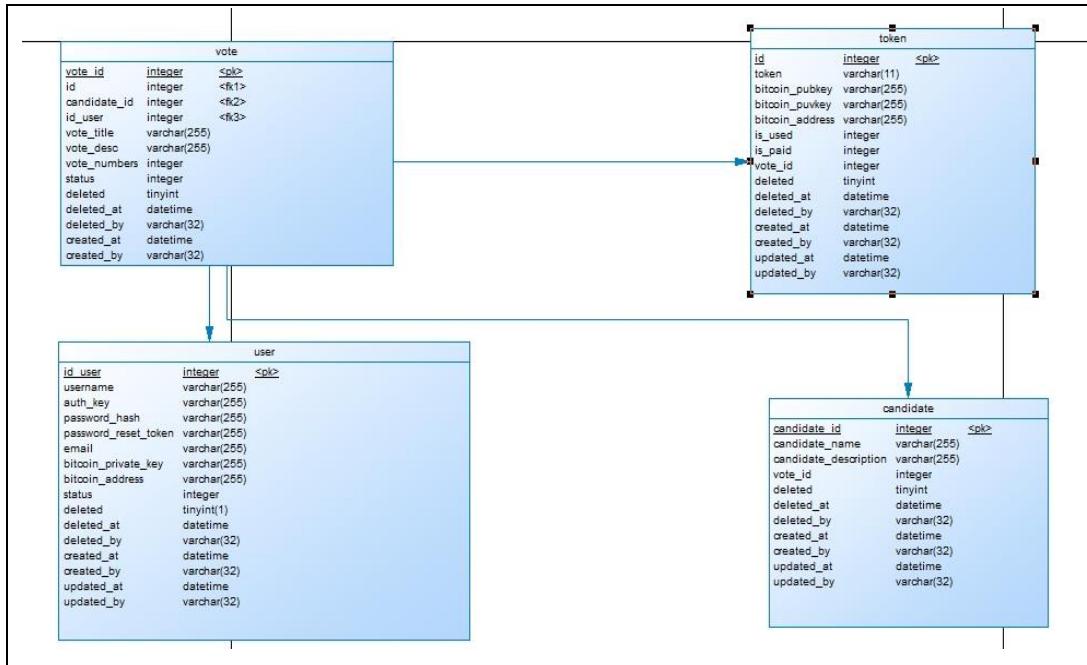
Pada bagian ini digambarkan CDM pembangunan sistem e-voting dapat dilihat pada Gambar 4.2 berikut.



Gambar 4.2. Conceptual Data Model

4.2.2 Physical Data Model (PDM)

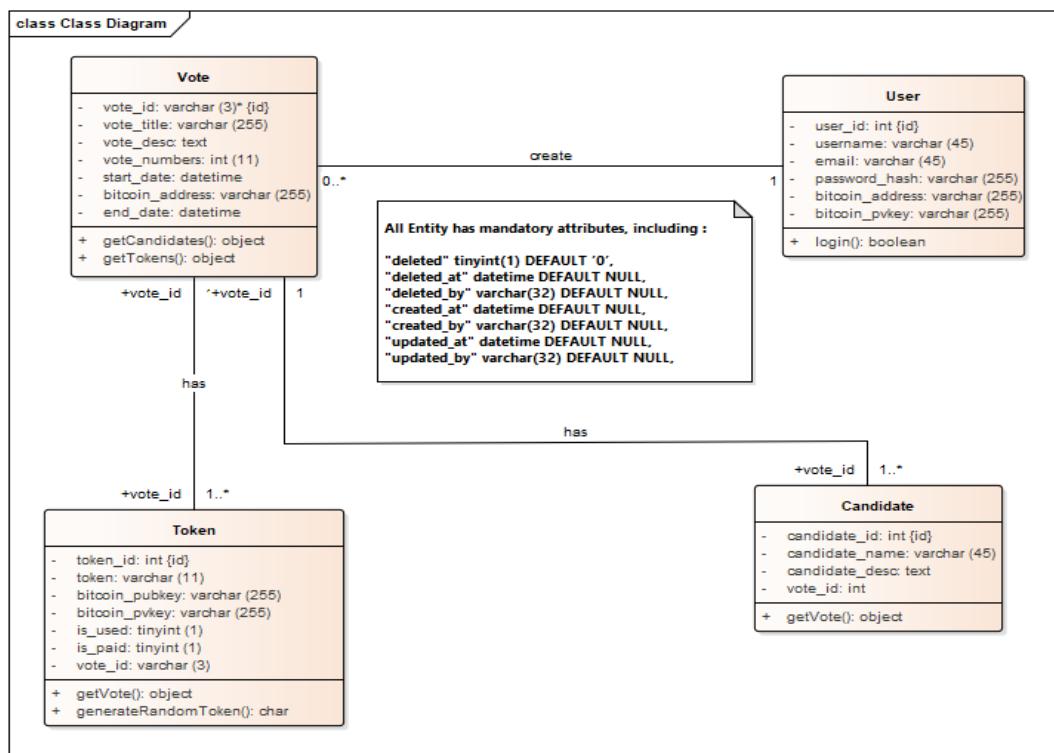
Pada bagian ini digambarkan PDM pembangunan sistem e-voting dapat dilihat pada Gambar 4.3 berikut.



Gambar 4.3. Physical Data Model

4.2.3 Class Diagram

Class diagram dari sistem yang akan dibangun dapat dilihat pada Gambar 4.4 berikut.



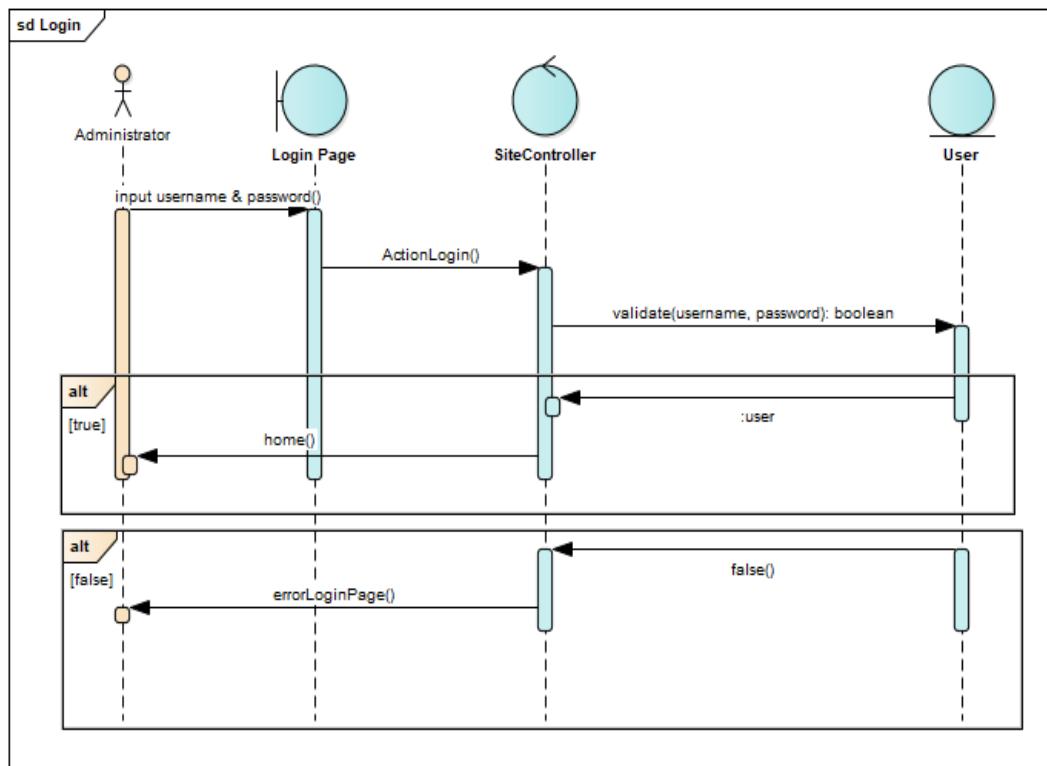
Gambar 4.4. Class Diagram

4.2.4 Sequence Diagram

Sequence diagram dari sistem e-voting menggunakan teknologi blockchain dapat dilihat sebagai berikut.

4.2.4.1 Login

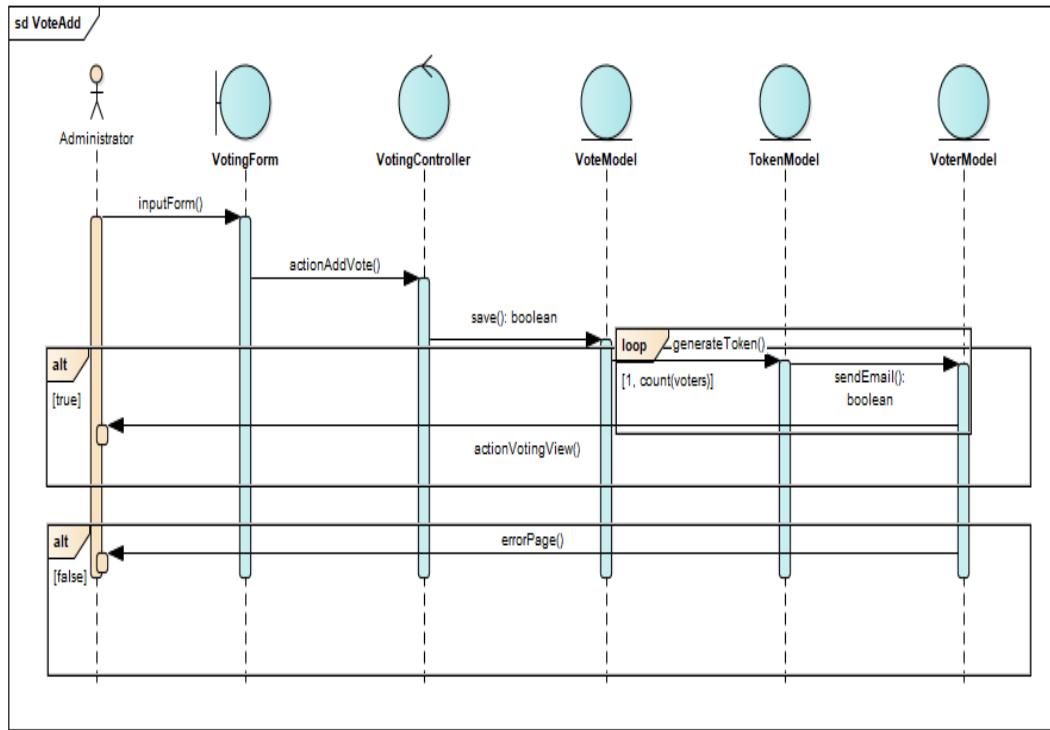
Sequence diagram pada *login* akan dijelaskan pada Gambar 4.5 berikut.



Gambar 4.5. Sequence Diagram Login

4.2.4.2 Membuat Voting

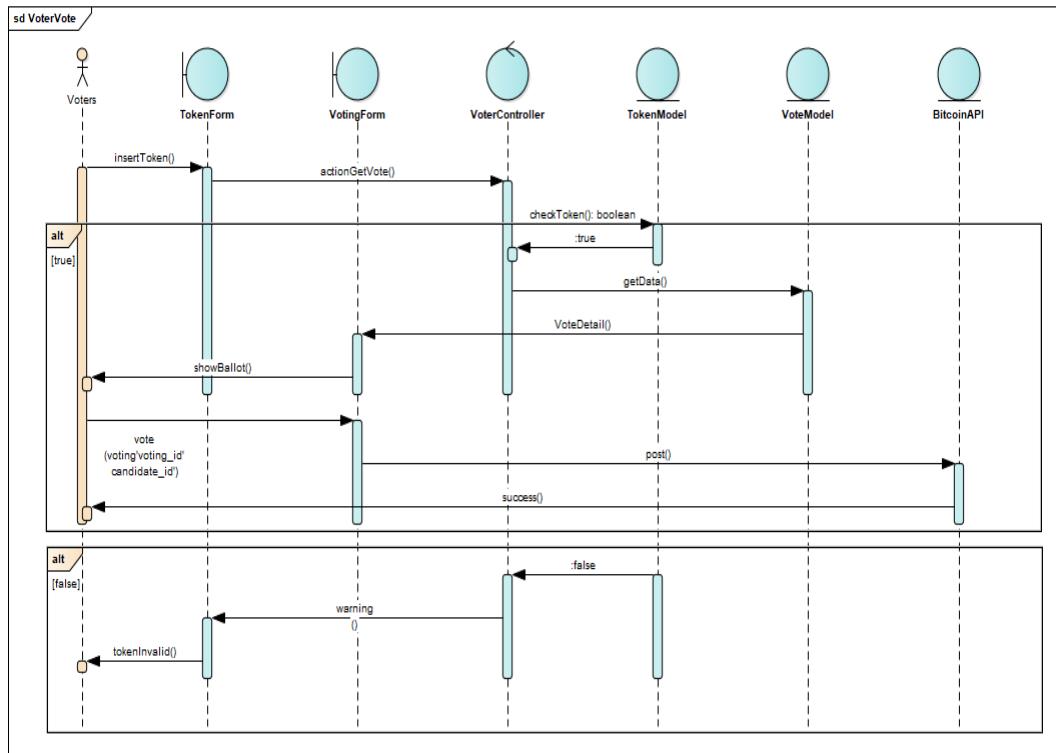
Sequence diagram membuat voting akan dijelaskan pada Gambar 4.6 berikut.



Gambar 4.6. Sequence Diagram Membuat Daftar Voting

4.2.4.3 Melakukan Voting

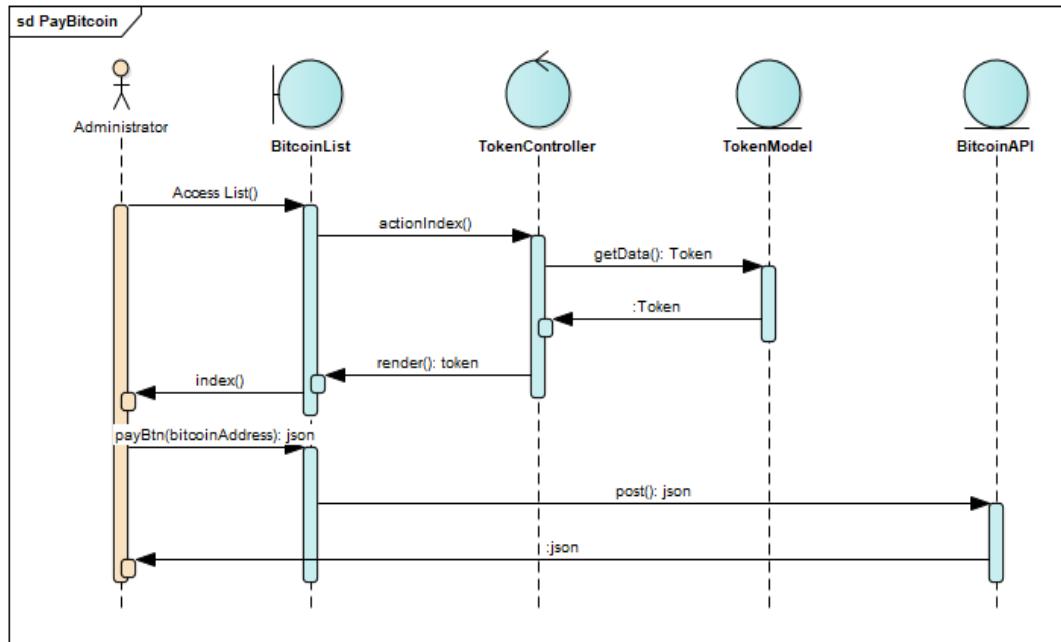
Sequence diagram melakukan voting akan dijelaskan pada Gambar 4.7 berikut.



Gambar 4.7. Sequence Diagram Melakukan Vote

4.2.4.4 Membayar Bitcoin Address

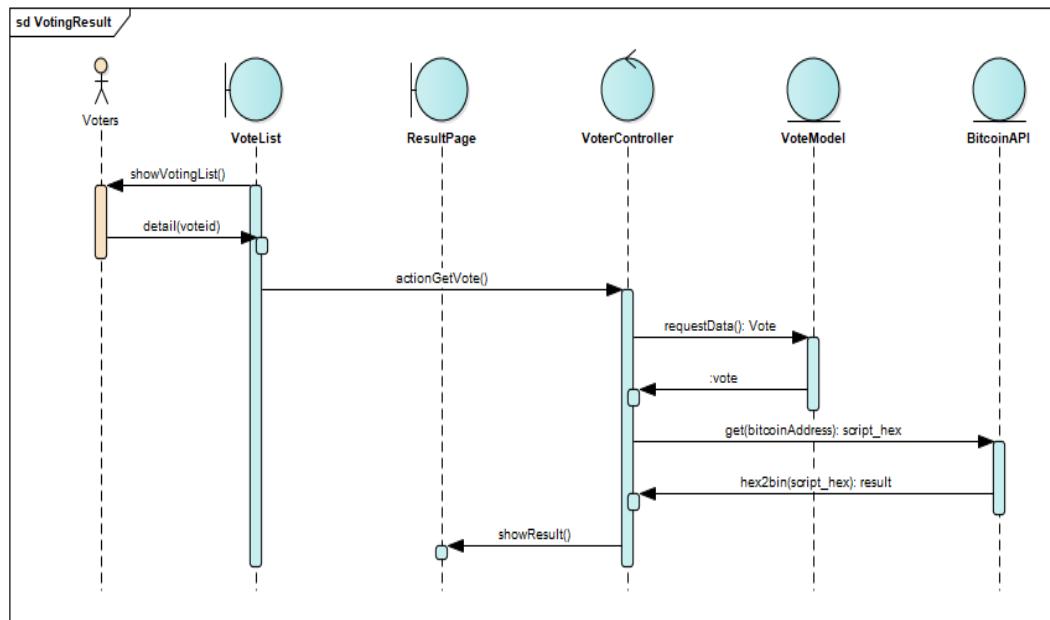
Sequence diagram membayar bitcoin address akan dijelaskan pada Gambar 4.8 berikut.



Gambar 4.8. Sequence Diagram Membayar Bitcoin Address

4.2.4.5 Melihat Hasil Voting

Sequence diagram melihat hasil voting akan dijelaskan pada Gambar 4.9 berikut.



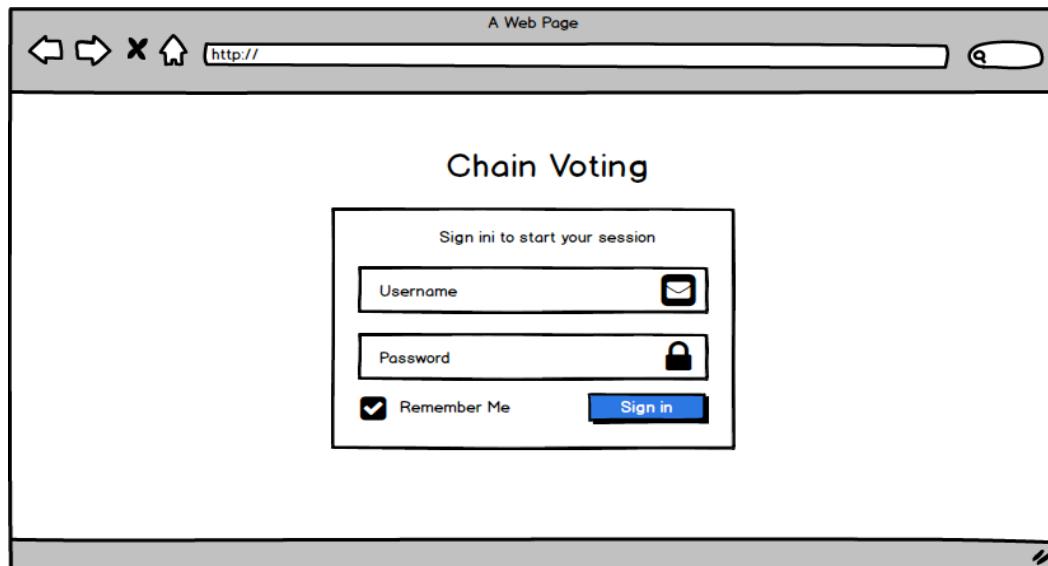
Gambar 4.9. Sequence Diagram Melihat Hasil Voting

4.2.5 Desain Antarmuka Sistem E-Voting menggunakan Blockchain

Pada subbab ini dijelaskan bagaimana desain antarmuka sistem yang akan dibangun pada web. Tampilan desain antarmuka diuraikan sebagai berikut :

1. Desain Sistem – Login Administrator

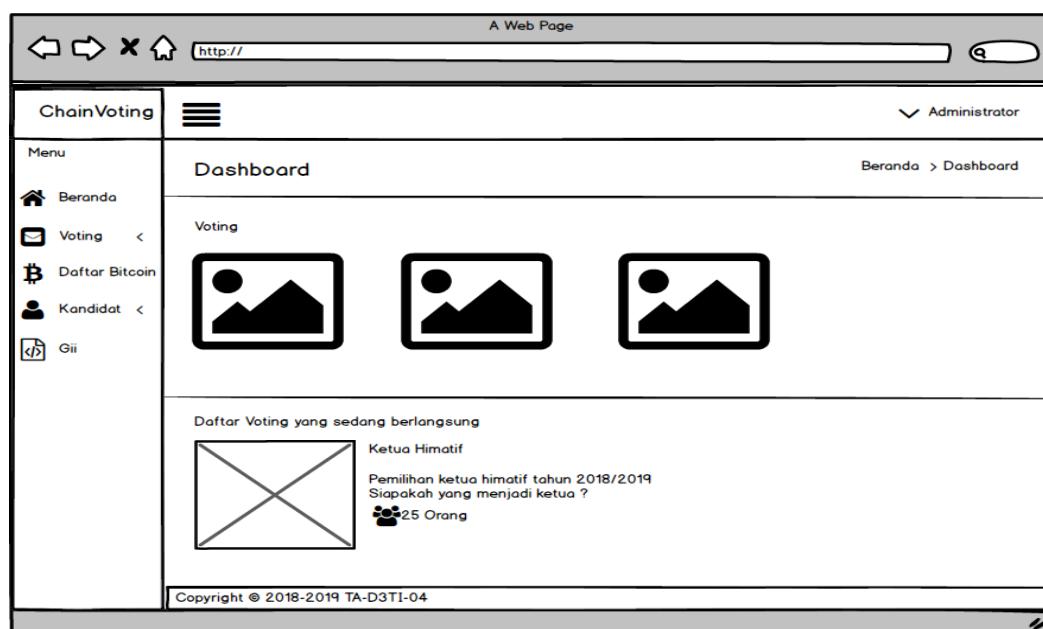
Tampilan desain sistem login untuk admin dapat dilihat pada Gambar 4.10 berikut.



Gambar 4.10. Desain Sistem – Login Administrator

2. Desain Sistem – Beranda

Tampilan desain sistem untuk beranda dapat dilihat pada Gambar 4.11 berikut.



Gambar 4.11. Desain Sistem – Beranda

3. Desain Sistem – Daftar Bitcoin Address

Tampilan desain sistem daftar bitcoin address dapat dilihat pada Gambar 4.12 berikut.

#	Bitcoin Address	Status	Voting	Operasi
1	Some text	Bitcoin Aktif	Some text	<button>Aktivasi Semua</button>

#	Bitcoin Address	Voting	Some text
1	Some text	Some text	

#	Bitcoin Address	Voting	Some text
1	Some text	Some text	

Gambar 4.12. Desain Sistem – Daftar Bitcoin Address

4. Desain Sistem – Membuat Daftar Kandidat

Tampilan desain sistem membuat daftar kandidat dapat dilihat pada Gambar 4.13 berikut.

Gambar 4.13. Desain Sistem – Membuat Daftar Kandidat

5. Desain Sistem – Daftar Kandidat

Tampilan desain sistem daftar kandidat untuk admin dapat dilihat pada Gambar 4.14 berikut.

A Web Page
http://

ChainVote Administrator

Kandidat Beranda > Kandidat

Voting Nama Kandidat

Daftar Bitcoin Vote to

Kandidat Pilih Vote

Daftar Kandidat

Tambah Kandidat

Gii

Cari Hapus

Menampilkan 1-1 dari 1 item.

#	Nama Kandidat	Deskripsi	Voting
1	Cici	· IPK : 4 · D3 Teknik Infrmatika 2016	Mahasiswa Teladan 2019

Copyright © 2018-2019 TA-D3TI-04

Gambar 4.14. Desain Sistem – Daftar Kandidat

6. Desain Sistem – Membuat Daftar Voting

Tampilan desain sistem membuat daftar voting dapat dilihat pada Gambar 4.15 berikut.

A Web Page
 http://

ChainVoting Administrator

Menu

- Voting
- Daftar Voting
- Tambah Voting
- Daftar Bitcoin
- Kandidat
- Gii

Tambah Vote Beranda > Votes > Tambah Votes

Nama Voting

Deskripsi

Tanggal Mulai Tanggal Berakhir

Kandidat Tambah Kandidat

Kandidat ke :1

Nama Kandidat

Deskripsi

File Pemilih

Browse

Silahkan memasukkan file excel daftar pemilih

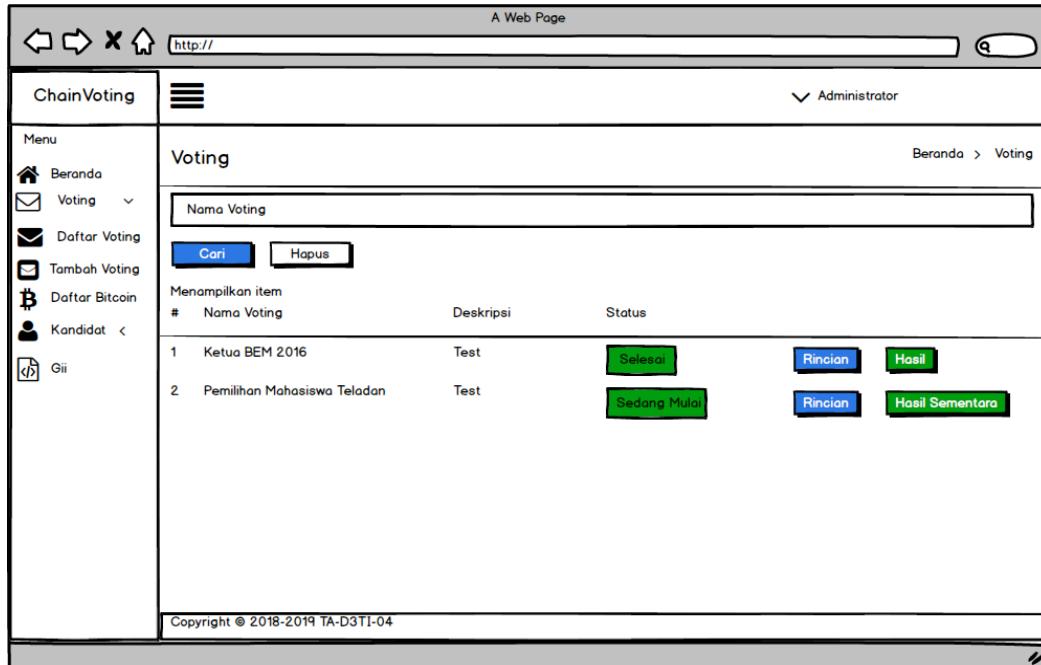
Tambah

Copyright © 2018-2019 TA-D3TI-04

Gambar 4.15. Desain Sistem – Membuat Daftar Voting

7. Desain Sistem – Daftar Voting

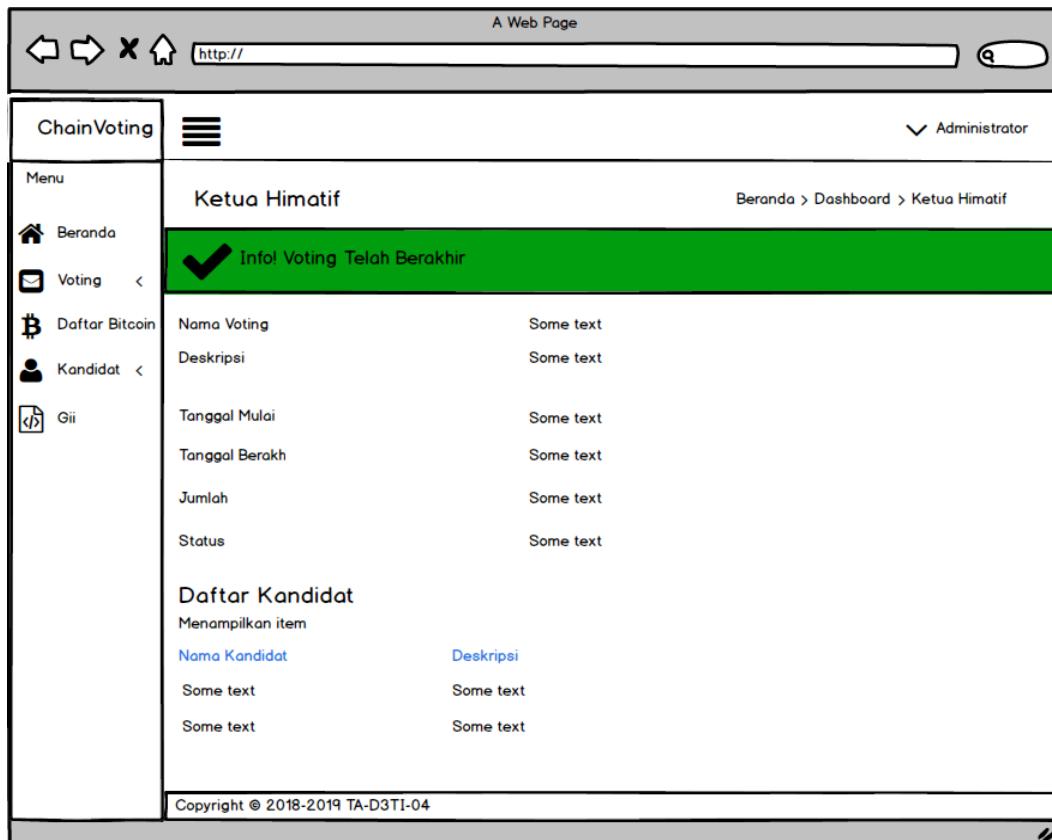
Tampilan desain sistem daftar voting dapat dilihat pada Gambar 4.16 berikut.



Gambar 4.16. Desain Sistem – Daftar Voting

8. Desain Sistem – Rincian Daftar Voting

Tampilan desain sistem rincian daftar voting dapat dilihat pada Gambar 4.17 berikut.



Gambar 4.17. Desain Sistem – Rincian Daftar Voting

9. Desain Sistem – Halaman Token

Tampilan desain sistem halaman token dapat dilihat pada Gambar 4.18 berikut.

Gambar 4.18. Desain Sistem – Halaman Token

10. Desain Sistem – Halaman Melakukan Vote

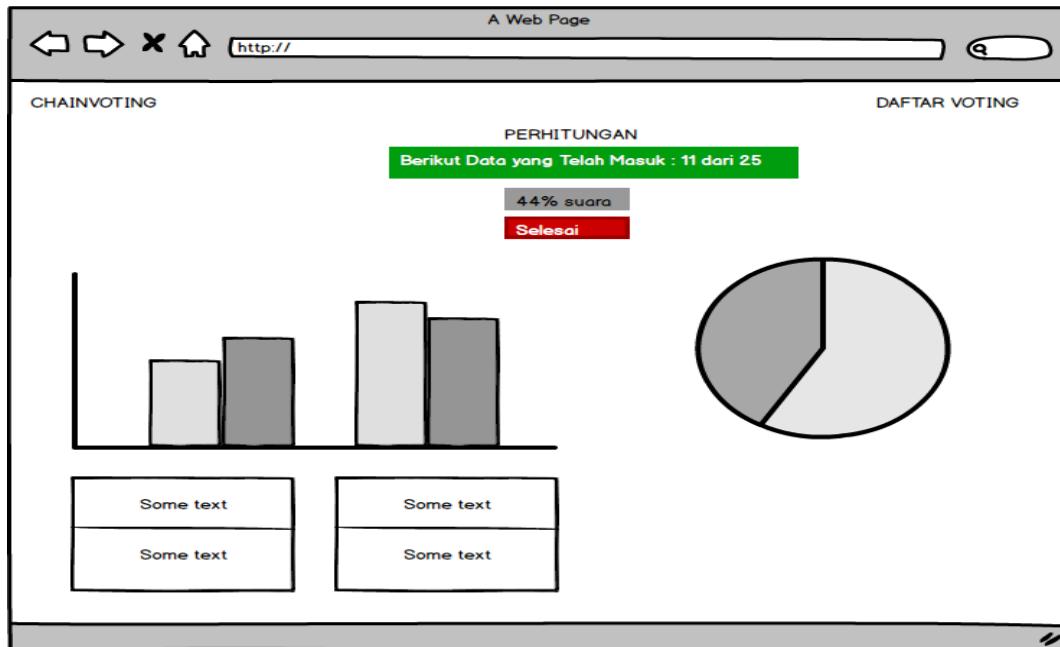
Tampilan desain sistem halaman untuk melakukan vote dapat dilihat pada Gambar 4.19 berikut.

Nama	Deskripsi	Aksi
Cici Munthe	<ul style="list-style-type: none"> • IPK : 4 • D3 Teknik Informatika 2016 	Vote
Jubelinda Silaen	<ul style="list-style-type: none"> • IPK : 3.9 • D3 Teknik Informatika 2016 	Vote

Gambar 4.19. Desain Sistem – Halaman Melakukan Vote

11. Desain Sistem – Hasil Voting

Tampilan desain sistem untuk hasil voting dapat dilihat pada Gambar 4.20 berikut.



Gambar 4.20. Desain Sistem – Hasil Voting

12. Desain Sistem – Daftar Voting untuk Voter

Tampilan desain sistem daftar voting untuk voter dapat dilihat pada Gambar 4.21 berikut.

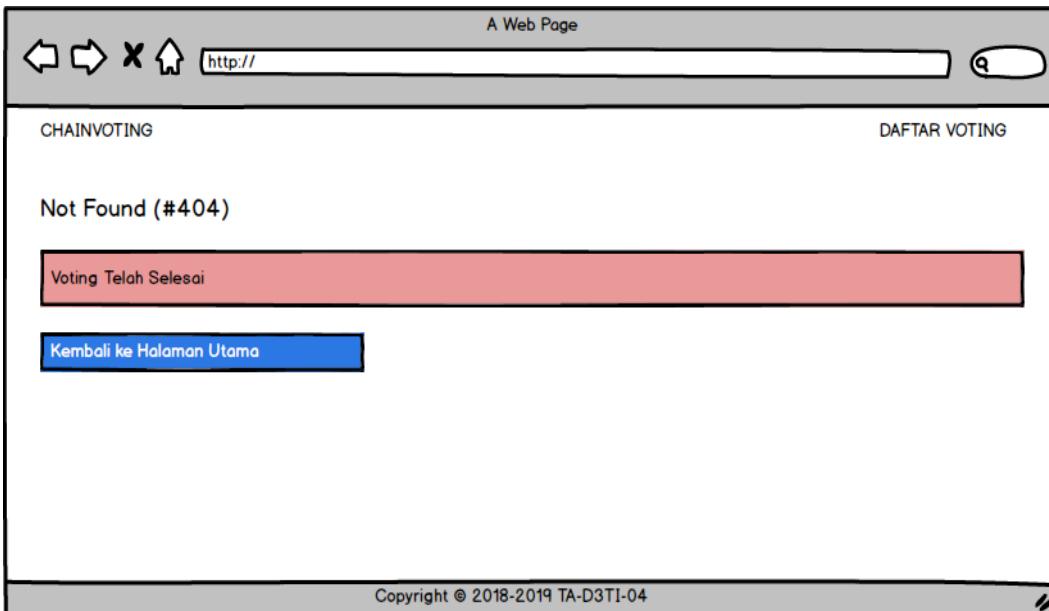
Beranda / Daftar Voting				
Menampilkan 1-2 dari 2 item				
#	Judul	Deskripsi	Status	Aksi
1	Pemilihan BEM 2016	Test1	Selesai	Hasil
2	Pemilihan Himapro	Test2	Selesai	Hasil

Copyright © 2018-2019 TA-D3TI-04

Gambar 4.21. Desain Sistem – Daftar Voting untuk Voter

13. Desain Sistem – Halaman Voting Selesai

Tampilan desain sistem halaman voting selesai dapat dilihat pada Gambar 4.22 berikut.



Gambar 4.22. Desain Sistem – Halaman Voting Selesai

4.2.6 Functional Requirement

Functional requirement akan dijelaskan pada Tabel 4.1 berikut.

Tabel 4.1. Functional Requirement

No	Main Function	Use Case	Keterangan
1	Fungsi Login	Login	Fungsi autentikasi digunakan oleh <i>admin</i> untuk masuk ke dalam aplikasi.
2	Fungsi Membuat Voting	Menambah Daftar Voting	Fungsi ini digunakan untuk menambah daftar voting.
3	Fungsi Menambah Kandidat	Menambah daftar kandidat	Fungsi ini digunakan untuk menambah daftar kandidat.
4	Fungsi Mendaftarkan Voter	Mendaftarkan voter	Fungsi ini digunakan untuk mendaftarkan

No	Main Function	Use Case	Keterangan
			voter
5	Fungsi Membayar Bitcoin Address	Membayar bitcoin address	Fungsi ini digunakan membayar bitcoin address dari daftar voter yang terdaftar
6	Fungsi Melakukan Voting	Melakukan voting	Fungsi ini digunakan untuk melakukan voting
7	Fungsi Melihat Hasil Voting	Melihat Hasil Voting	Fungsi ini digunakan melihat detail hasil voting.

BAB 5

IMPLEMENTASI

Pada bab ini akan dijelaskan deskripsi umum sistem yang meliputi kebutuhan implementasi, tahapan implementasi, dan implementasi aplikasi.

5.1 Implementasi

Pada bab ini akan dijelaskan mengenai kebutuhan implementasi, batasan implementasi, dan tahapan implementasi.

5.1.1 Kebutuhan Implementasi

Pada subbab ini akan dijelaskan kebutuhan *tools* yang digunakan dalam pembangunan aplikasi. Dibutuhkan beberapa *tools hardware* dan *software* dalam mendukung dan mempermudah proses pembangunan aplikasi seperti untuk menjalankan aplikasi, menyimpan data, penggeraan kode program, dan lain sebagainya. Adapun spesifikasi *hardware* dan *software* yang dibutuhkan dalam pembangunan sistem e-voting menggunakan teknologi blockchain. Spesifikasi perangkat keras yang digunakan pada pengimplementasian akan dijelaskan pada Tabel 5.1 berikut ini.

Tabel 5.1. Spesifikasi Hardware dan Software

No	Hardware	Spesifikasi
1	Processor	Intel ® Core™ i5-3230M CPU @ 2.60GHz (4 CPUs), ~2.6GHz
2	RAM	8GB

No	Software	Spesifikasi
1	Operating System	Windows 10
2	Development Tools	Php Storm
3	Programming Language	PHP, Javascript
4	Database Tools	SQLyog
5	Database	MySQL
6	Framework	Yii2
7	Design Tools	Enterprise Architect, Balsamiq Mockups 3, Bizagi, Power Designer 15.2

8	Library	Bitcoin PHP dan Bitcoin JS
8	Testnet Bitcoin	API Chain.so
9	Paket Office	Microsoft Office 2016

5.1.2 Tahapan Implementasi

Pada subbab ini akan dijelaskan persiapan sebelum pelaksanaan implementasi sistem e-voting menggunakan teknologi blockchain. Berikut akan dijelaskan tahapannya :

1. Instalasi tools/software

Instalasi tools/software yang dilakukan pada laptop yang akan digunakan sebagai media untuk membuat kode program dan menjalankan program dengan spesifikasi pada subbab 5.1.1.

2. Melakukan penulisan *code* program untuk implementasi sistem e-voting

Setelah instalasi tools dan software dilakukan, maka selanjutnya akan dilakukan penulisan *code* program pada editor yang sudah diinstalasi. Setelah *source code* dituliskan, maka akan dilakukan proses menghubungkan sistem e-voting dengan teknologi blockchain yaitu layanan API Blockchain. Source code dapat dilihat pada Lampiran 1-Source Code Sistem.

Tahapan dalam implementasi yang akan dilaksanakan oleh tim peneliti adalah sebagai berikut :

1. Tahap pertama adalah melakukan analisis pada sistem e-voting menggunakan teknologi blockchain. Tim peneliti akan menganalisis bagaimana sistem e-voting berinteraksi/terhubung dengan teknologi blockchain. Untuk mempercepat proses *development* sistem e-voting, tim peneliti menggunakan salah satu layanan API Blockchain yaitu API SoChain.

2. Tahap kedua adalah implementasi aplikasi. Dalam tahap ini tim peneliti akan melakukan implementasi untuk membuat sistem e-voting yang dapat dijalankan pada platform web. Tahap ini akan menghasilkan aplikasi web yang memiliki fungsi untuk melakukan

vote, mengelola daftar kandidat, membuat voting, mendaftarkan voter, dan melihat hasil voting.

3. Tahap ketiga adalah menghubungkan sistem e-voting dengan layanan API Blockchain. Layanan ini digunakan untuk membuat dan mengambil transaksi voting di bitcoin testnet. Selanjutnya akan dilakukan perhitungan hasil voting.
4. Tahap keempat adalah pengujian terhadap aplikasi. Dalam tahap ini aplikasi yang telah dihasilkan dari tahap sebelumnya akan diuji apakah sudah sesuai dengan hasil yang diharapkan dan output yang dihasilkan berjalan dengan baik dan tidak memiliki *error*.

5.2 Implementasi Aplikasi

Pada subbab ini dijelaskan mengenai aplikasi yang diimplementasikan dalam pelaksanaan Tugas Akhir. Sistem e-voting menggunakan teknologi Blockchain yang dibangun merupakan aplikasi yang berbasis web yang dibangun menggunakan PHP, JavaScript dengan *framework yii2*. Untuk menghubungkan aplikasi sistem informasi ke database menggunakan SQL Server. Sedangkan untuk menghubungkan sistem e-voting dengan teknologi blockchain menggunakan layanan API Blockchain. Layanan ini digunakan untuk membuat transaksi voting dan mengambil transaksi tersebut berdasarkan bitcoin address yang dimiliki voter.

BAB 6

PENGUJIAN

Pada subbab ini akan dijelaskan mengenai pengujian yang akan dilakukan pada sistem e-voting menggunakan teknologi blockchain yang terdiri dari prosedural pengujian, tujuan pengujian, persiapan *software* dan *hardware* untuk pengujian, dan *scenario* pengujian.

6.1 Prosedural Pengujian

Persiapan prosedural yang harus dilakukan sebelum tahap pengujian tehadap aplikasi adalah mempersiapkan tools untuk menjalankan aplikasi seperti Laptop dan aplikasi yang akan diuji. Tim peneliti menggunakan metode wawancara kepada para responden untuk melakukan evaluasi pada sistem e-voting menggunakan teknologi blockchain yang sudah diintegrasikan ke aplikasi web. Responden yang melakukan pengujian adalah mahasiswa yang pernah melakukan pemilihan di Institut Teknologi Del. Jumlah sampel yang menjadi pengguna sistem e-voting untuk pengujian adalah 28 orang dari prodi Diploma 3 Teknik Informatika angkatan 2016.

Responden tersebut diharapkan dapat memberikan tanggapan mengenai sistem e-voting menggunakan teknologi blockchain apakah sudah sesuai dengan hasil yang diharapkan dan keamanan voting sudah meliputi aspek *accuracy*, *invulnerability*, *privacy*, dan *verifiability*. Dalam memberikan evaluasi baik berupa komentar, saran, dan tanggapan, Tim peneliti melakukannya dengan cara memberikan aplikasi kepada responden, kemudian responden akan menguji setiap fungsi yang telah ditentukan pada sistem e-voting. Setelah melakukan pengujian setiap responden akan memberikan penilaian mengenai semua fungsi yang telah dijalankan mulai dari fungsi melakukan voting, melihat hasil voting, verifikasi voting, mengelola daftar kandidat, membuat daftar voter, dan mendaftarkan voter, memulai voting, dan menghentikan voting.

6.2 Tujuan Pengujian

Tujuan dari proses pengujian yang dilakukan pada sistem e-voting menggunakan teknologi blockchain adalah sebagai berikut :

1. Pengujian dilakukan untuk memastikan bahwa aplikasi dapat berjalan dengan baik dan tidak memiliki *error*.
2. Pengujian dilakukan untuk memvalidasi apakah keamanan data voting menggunakan teknologi blockchain sudah mencakup aspek *accuracy*, *invulnerability*, *privacy*, dan *verifiability*.
3. Pengujian dilaksanakan untuk memastikan bahwa aplikasi telah memenuhi kebutuhan pengguna/*client*.

6.3 Persiapan Hardware dan Software untuk Pengujian

Persiapan hardware yang diperlukan untuk pengujian aplikasi adalah sebagai berikut

1. Mempersiapkan laptop yang digunakan sebagai server yang memiliki spesifikasi pada subbab 5.1.1.
2. Memastikan laptop dapat mengakses aplikasi.

Persiapan software yang diperlukan untuk pengujian adalah sistem e-voting menggunakan teknologi blockchain yang sudah dibuat dan dapat menjalankan semua fungsi yang telah ditentukan seperti melakukan voting, melihat hasil voting, verifikasi voting, mengelola daftar kandidat, membuat daftar voter, dan mendaftarkan voter, memulai voting, dan menghentikan voting.

6.4 Scenario Pengujian

Berikut akan dijelaskan scenario pengujian pada fungsi yang terdapat pada sistem berdasarkan *use case scenario*.

1. Skenario Pengujian Aunthentication

Pengujian *authentication* dilakukan untuk memastikan bahwa admin dapat masuk ke dalam sistem. Hasil pengujian dapat dilihat pada Tabel 6.1 berikut.

Tabel 6.1. Pengujian Aunthentication

Nama Kasus Uji	Authentication pada Sistem E-Voting menggunakan Teknologi Blockchain
Tujuan	Menguji apakah admin dapat masuk ke dalam sistem
Deskripsi	Fungsi ini akan menyimpan data admin
Kondisi Awal	Admin telah terotentikasi dan berada pada tampilan awal Home
Skenario Uji	
1. Admin membuka halaman login dan mengisi data yang diperlukan	

seperti username dan password 2. Admin masuk ke dalam sistem Chain Vote			
Kriteria Evaluasi Hasil			
Admin berhasil masuk ke dalam sistem dan data admin disimpan di dalam sistem			
Kasus dan Hasil Uji (Data Normal)			
Data masukan	Yang diharapkan	Pengamatan	Kesimpulan
Admin memasukkan <i>username</i> dan <i>password</i>	Admin berhasil masuk ke dalam sistem	Sesuai yang diharapkan	Diterima
Kasus dan Hasil Uji Coba (Data Tidak Normal)			
Admin tidak memasukkan <i>username</i> atau <i>password</i> atau keduanya	Tetap di halaman <i>Login</i>	Sesuai yang diharapkan	Diterima
Catatan			
Admin berhasil masuk ke dalam sistem sesuai dengan <i>rolenya</i> masing-masing			

2. Skenario Pengujian Membuat Voting

Pengujian membuat voting dilakukan untuk memastikan bahwa admin dapat memasukkan daftar voting. Pada saat admin membuat voting admin juga menambahkan daftar kandidat, memasukkan waktu mulai dan selesai voting, Hasil pengujian dapat dilihat pada Tabel 6.2 berikut.

Tabel 6.2. Pengujian Membuat Daftar Voting

Nama Kasus Uji	Membuat voting pada Sistem E-Voting menggunakan Teknologi Blockchain
Tujuan	Menguji apakah admin dapat memasukkan daftar voting
Deskripsi	Fungsi ini akan menyimpan dan menampilkan daftar voting pada sistem
Kondisi Awal	Admin telah terotentikasi dan berada pada tampilan awal beranda
Skenario Uji	
1. Admin membuka satu menu : Voting 2. Admin memilih satu menu : Tambah voting 3. Admin memilih menu : Daftar voting 4. Admin memilih menu : Rincian	

<p>5. Admin memilih menu : Hasil</p>			
Kriteria Evaluasi Hasil			
<ol style="list-style-type: none"> 1. Admin berhasil membuka menu voting 2. Admin berhasil menambahkan voting pada sistem 3. Admin berhasil memasukkan waktu mulai dan selesai voting 4. Admin berhasil menambahkan kandidat pada sistem 5. Admin berhasil menambahkan daftar voter pada sistem 6. Admin berhasil membuka daftar voting pada sistem 7. Admin berhasil membuka rincian voting pada sistem 8. Admin berhasil melihat status voting pada sistem 9. Admin berhasil membuka hasil voting pada sistem 			
Kasus dan Hasil Uji (Data Normal)			
Data masukan	Yang diharapkan	Pengamatan	Kesimpulan
1. Admin memilih menu voting	Menu voting akan ditampilkan	Sesuai yang diharapkan	Diterima
2. Admin memilih menu tambah voting dan mengisi form tambah vote pada form yang telah disediakan yaitu nama, deskripsi, tanggal mulai, tanggal berakhir voting, mengisi form kandidat yaitu nama kandidat dan deskripsi, mendaftarkan pemilih dengan memasukkan file excel daftar pemilih dan menekan tombol tambah	Daftar vote dan daftar kandidat akan bertambah dan ditampilkan serta file pemilih akan ditambahkan	Sesuai yang diharapkan	Diterima
3. Admin memilih menu daftar	Daftar voting akan	Sesuai yang diharapkan	Diterima

voting	ditampilkan		
4. Admin memilih menu rincian daftar voting yang telah dipilih pada daftar voting	Rincian daftar voting yang telah dipilih akan ditampilkan yaitu nama voting, deskripsi, tanggal mulai, tanggal berakhir, jumlah, dan status voting serta daftar kandidat	Sesuai yang diharapkan	Diterima
5. Admin memilih hasil pada daftar voting yang telah dipilih	Hasil voting pada daftar voting yang telah dipilih akan ditampilkan	Sesuai yang diharapkan	Diterima

Kasus dan Hasil Uji Coba (Data Tidak Normal)

1. Admin memilih menu save namun tidak mengisi form	Sistem akan menampilkan <i>message error</i> yaitu nama voting tidak boleh kosong, tanggal mulai tidak boleh kosong, tanggal berakhir tidak boleh kosong, nama kandidat tidak boleh kosong, file import tidak boleh kosong dan data tidak akan bertambah dan ditampilkan	Sesuai yang diharapkan	Diterima
2. Admin memasukkan file excel daftar pemilih dimana pada file excel	Sistem akan melakukan pengecekan pada file excel daftar pemilih. Jika		

ada alamat email yang sama dengan voter lainnya dimasukkan pada file excel	pada file excel ada alamat email yang sama maka sistem tidak akan mendaftarkan salah satu voter yang memiliki alamat email yang sama dengan voter lainnya. Jadi sistem hanya mendaftarkan salah satu email dari kedua email yang sama yaitu alamat email yang pertama		
Catatan			
Admin berhasil membuat voting			

3. Skenario Pengujian Melakukan Voting

Pengujian melakukan voting dilakukan untuk memastikan bahwa voter dapat melakukan voting. Hasil pengujian dapat dilihat pada Tabel 6.3 berikut.

Tabel 6.3. Pengujian Melakukan Vote

Nama Kasus Uji	Melakukan vote pada Sistem E-Voting menggunakan Teknologi Blockchain
Tujuan	Menguji apakah voter dapat melakukan voting
Deskripsi	Fungsi ini akan menyimpan hasil voting dan menampilkan hasil voting
Kondisi Awal	Voter telah menerima email berisi link untuk melakukan voting dan alamat token
Skenario Uji	
<ol style="list-style-type: none"> 1. Admin menambahkan voting dengan mengisi form tambah voting seperti Nama Voting, Deskripsi, Tanggal Mulai, Tanggal Berakhir, mengisi form kandidat seperti Nama Kandidat, Deskripsi dan mendaftarkan voter dengan memasukkan file excel daftar pemilih 2. Admin membuka daftar bitcoin untuk membayar bitcoin address dari daftar voter yang telah didaftarkan agar statusnya menjadi “sudah dibayar” 3. Admin membuka daftar voting untuk melihat nama voting, deskripsi, status, menu rincian, menu hasil 	

<p>4. Admin membuka menu rincian pada halaman daftar voting 5. Admin membuka menu hasil pada halaman daftar voting 6. Voter membuka email berisi token dan link untuk melakukan voting 7. Voter membuka link voting dan mengcopy alamat token 8. Voter memasukkan alamat token pada form memasukkan token 9. Voter melihat informasi detail kandidat seperti nama kandidat, deskripsi dan aksi untuk menekan tombol vote 10. Voter melakukan voting dengan mengklik tombol vote</p>			
Kriteria Evaluasi Hasil			
<p>1. Admin berhasil menambahkan daftar voting pada sistem 2. Admin berhasil menambahkan daftar kandidat pada sistem 3. Admin berhasil mendaftarkan voter dan mengirimkan link voting dan alamat token kepada user yang didaftarkan pada sistem 4. Admin berhasil membayar bitcoin address dari daftar voter yang telah didaftarkan pada sistem 5. Admin berhasil membuka rincian daftar voting pada halaman daftar voting yaitu nama voting, deskripsi, tanggal mulai, tanggal berakhir, jumlah, status voting, dan daftar kandidat 6. Admin berhasil membuka hasil voting pada halaman daftar voting 7. Voter berhasil membuka email untuk voting yang berisi alamat token dan link untuk melakukan voting pada sistem 8. Voter berhasil membuka link voting dan memasukkan alamat token pada halaman form token yang disediakan pada sistem 9. Sistem berhasil memvalidasi alamat token yang dimasukkan oleh voter 10. Voter berhasil melakukan voting pada sistem 11. Sistem berhasil menyimpan hasil voting dan menampilkan hasil voting pada sistem 12. Sistem berhasil menampilkan status waktu voting pada halaman hasil voting 13. Sistem berhasil menampilkan waktu voting pada halaman daftar voting untuk voter</p>			
Kasus dan Hasil Uji (Data Normal)			
Data masukan	Yang diharapkan	Pengamatan	Kesimpulan
1. Admin menambahkan daftar voting dengan mengisi form tambah vote yaitu nama voting, deskripsi, mengatur tanggal mulai, tanggal	Daftar voting, daftar kandidat akan bertambah dan ditampilkan dan file daftar voter akan bertambah	Sesuai dengan yang diharapkan	Diterima

berakhir, mengisi form kandidat yaitu nama kandidat, deskripsi, dan memasukkan daftar voter dengan memasukkan file excel daftar pemilih dan memilih tombol tambah			
2. Admin membuka daftar bitcoin untuk membayar bitcoin address dari daftar voter telah didaftarkan dan menekan tombol bayar	Sistem akan membayar bitcoin address dari daftar voter telah didaftarkan dan status bitcoin address akan diubah menjadi menjadi “sudah dibayar”	Sesuai dengan yang diharapkan	Diterima
3. Admin membuka menu daftar voting	Sistem akan menampilkan masing-masing nama voting, deskripsi, status voting, menu rincian daftar voting, dan menu hasil untuk melihat hasil voting	Sesuai dengan yang diharapkan	Diterima
4. Voter membuka menu rincian pada halaman daftar voting	Sistem akan menampilkan rincian daftar voting yaitu nama voting, deskripsi, tanggal mulai, tanggal berakhir, jumlah voter yang terdaftar, dan status voting	Sesuai dengan yang diharapkan	Diterima
5. Voter membuka menu hasil pada halaman daftar voting	Sistem akan menampilkan hasil perhitungan voting dan status waktu voting	Sesuai dengan yang diharapkan	Diterima

6. Voter membuka emailnya untuk melihat token dan link untuk melakukan voting	Sistem akan menampilkan email berdasarkan alamat email yang telah dimasukkan admin	Sesuai dengan yang diharapkan	Diterima
7. Voter membuka link voting dan mencopy alamat token	Sistem akan menampilkan form untuk memasukkan alamat token	Sesuai dengan yang diharapkan	Diterima
8. Voter memasukkan alamat token	Sistem akan memverifikasi alamat token yang dimasukkan oleh voter, jika alamat token yang dimasukkan valid maka voter dapat masuk ke halaman voting, namun jika alamat token yang dimasukkan voter tidak valid maka sistem akan menampilkan <i>message error</i> "Maaf, Token anda tidak valid" dan voter tidak akan masuk ke halaman voting	Sesuai dengan yang diharapkan	Diterima
9. Voter melakukan voting dengan menekan tombol vote	Sistem akan menampilkan detail hasil voting yaitu jumlah data voting yang telah masuk (jumlah seluruh voter yang telah melakukan voting dan jumlah voter yang telah terdaftar), hasil voting pada masing-masing kandidat dalam diagram lingkaran, jumlah voter yang memilih masing-masing kandidat,	Sesuai dengan yang diharapkan	Diterima

	dan status waktu voting		
Kasus dan Hasil Uji Coba (Data Tidak Normal)			
1. Voter memilih tombol tambah namun tidak memasukkan nama voting pada form tambah vote	Sistem akan menampilkan <i>message error</i> yaitu “Nama Voting tidak boleh kosong” dan data tidak akan dikirimkan	Sesuai dengan yang diharapkan	Diterima
2. Voter memilih tombol tambah namun tidak memasukkan tanggal mulai voting pada form tambah vote	Sistem akan menampilkan <i>message error</i> yaitu “Tanggal Mulai tidak boleh kosong” dan data tidak akan dikirimkan	Sesuai dengan yang diharapkan	Diterima
3. Voter memilih tombol tambah namun tidak memasukkan tanggal berakhir voting pada form tambah vote	Sistem akan menampilkan <i>message error</i> yaitu “Tanggal Berakhir tidak boleh kosong” dan data tidak akan dikirimkan	Sesuai dengan yang diharapkan	Diterima
4. Voter memilih tombol tambah namun tidak memasukkan nama kandidat pada form tambah kandidat	Sistem akan menampilkan <i>message error</i> yaitu “Nama Kandidat tidak boleh kosong” dan data tidak akan dikirimkan	Sesuai dengan yang diharapkan	Diterima
5. Voter memilih tombol tambah namun tidak memasukkan file	Sistem akan menampilkan <i>message error</i> yaitu “File import	Sesuai dengan yang diharapkan	Diterima

excel daftar pemilih	tidak boleh kosong” dan data tidak akan dikirimkan		
6. Voter memasukkan alamat token yang salah	Sistem akan menampilkan <i>message error</i> yaitu “Maaf, token anda tidak valid”	Sesuai dengan yang diharapkan	Diterima
7. Voter memasukkan kembali alamat token yang telah digunakan	Sistem akan menampilkan <i>message error</i> yaitu “Maaf, Token anda telah digunakan atau belum diizinkan untuk voting”	Sesuai dengan yang diharapkan	Diterima
8. Admin memasukkan file excel daftar pemilih dimana pada file excel ada alamat email yang sama dengan voter lainnya dimasukkan pada file excel	Sistem akan melakukan pengecekan pada file excel daftar pemilih. Jika admin mendaftarkan alamat email yang sama maka sistem tidak akan mendaftarkan salah satu voter yang memiliki alamat email yang sama dengan voter lainnya. Jadi sistem hanya mendaftarkan salah satu email dari kedua email yang sama yaitu alamat email yang pertama	Sesuai dengan yang diharapkan	Diterima
9. Voter melakukan voting namun status voting telah selesai	Sistem akan menampilkan <i>message error</i> yaitu voting telah selesai	Sesuai dengan yang diharapkan	Diterima
Catatan			
Voter berhasil melakukan voting			

4. Skenario Pengujian Melihat Hasil Voting

Pengujian melihat hasil voting dilakukan untuk memastikan bahwa voter dapat melihat hasil voting. Hasil pengujian dapat dilihat pada Tabel 6.4 berikut.

Tabel 6.4. Pengujian Melihat Hasil Voting

Nama Kasus Uji	Melihat hasil voting pada Sistem E-Voting menggunakan Teknologi Blockchain					
Tujuan	Menguji apakah voter dapat melihat detail hasil voting					
Deskripsi	Fungsi ini akan menampilkan hasil voting					
Kondisi Awal	Voter telah melakukan voting					
Skenario Uji						
<ol style="list-style-type: none"> 1. Voter telah mengakses link voting dari email 2. Voter membuka daftar voting 3. Voter memilih salah satu item vote pada daftar voting yang akan dilihat hasilnya 4. Voter memilih tombol Hasil 						
Kriteria Evaluasi Hasil						
<ol style="list-style-type: none"> 1. Voter berhasil membuka link voting 2. Voter berhasil membuka daftar voting pada sistem 3. Voter berhasil memilih salah satu item vote pada daftar voting untuk dilihat hasilnya pada sistem 4. Voter berhasil melihat hasil voting pada sistem 						
Kasus dan Hasil Uji (Data Normal)						
Data masukan	Yang diharapkan	Pengamatan	Kesimpulan			
1. Voter membuka link voting dari email	Sistem akan menampilkan halaman hasil voting	Sesuai yang diharapkan	Diterima			
2. Voter membuka daftar voting	Sistem akan menampilkan daftar voting	Sesuai yang diharapkan	Diterima			
3. Voter memilih salah satu item vote dan memilih tombol hasil	Sistem akan menampilkan detail hasil voting yaitu jumlah data voting yang telah masuk (jumlah voter yang telah melakukan voting dan jumlah voter yang telah terdaftar), hasil	Sesuai yang diharapkan	Diterima			

	voting masing-masing kandidat dalam diagram lingkaran, jumlah voter yang memilih masing-masing kandidat, dan status waktu voting		
Kasus dan Hasil Uji Coba (Data Tidak Normal)			
Catatan			
Voter berhasil melihat hasil voting pada sistem			

5. Skenario Pengujian Membayar Bitcoin Address

Pengujian membayar bitcoin dilakukan untuk memastikan bahwa admin dapat membayar bitcoin address pada sistem ChainVote. Hasil pengujian dapat dilihat pada Tabel 6.5 berikut.

Tabel 6.5. Pengujian Membayar Bitcoin Address

Nama Kasus Uji	Membayar Bitcoin Address pada Sistem E-Voting menggunakan Teknologi Blockchain
Tujuan	Menguji apakah admin dapat membayar bitcoin address pada sistem
Deskripsi	Fungsi ini akan menyimpan dan menampilkan bitcoin address pada sistem
Kondisi Awal	Admin telah terotentikasi dan berada pada tampilan awal beranda
Skenario Uji	
<ol style="list-style-type: none"> 1. Admin telah mendaftarkan voter pada daftar voting 2. Admin memilih menu : daftar bitcoin 3. Admin memilih satu menu : Aktivasi 4. Admin memilih satu menu : close 	
Kriteria Evaluasi Hasil	
<ol style="list-style-type: none"> 1. Admin berhasil mendaftarkan daftar voter 2. Admin berhasil membuka daftar bitcoin pada sistem 3. Admin berhasil membayar bitcoin address masing-masing voter yang telah terdaftar pada sistem 4. Admin berhasil menutup atau keluar dari sistem 	
Kasus dan Hasil Uji (Data Normal)	

Data masukan	Yang diharapkan	Pengamatan	Kesimpulan
1. Admin memilih menu daftar bitcoin	Daftar bitcoin akan ditampilkan	Sesuai yang diharapkan	Diterima
2. Admin memilih operasi aktivasi pada bitcoin address	Status bitcoin address dari masing-masing pemilih yang telah didaftarkan menjadi “aktif”	Sesuai yang diharapkan	Diterima
3. Admin memilih menu close	Admin akan keluar dari sistem	Sesuai yang diharapkan	Diterima
Kasus dan Hasil Uji Coba (Data Tidak Normal)			
1. Admin tidak mendaftarkan voter	Sistem tidak akan menampilkan daftar bitcoin address	Sesuai yang diharapkan	Diterima
2. Admin tidak membayar bitcoin address dari voter yang telah terdaftar	Voter tidak akan dapat melakukan voting	Sesuai yang diharapkan	Diterima
Catatan			
Admin berhasil membayar bitcoin address dari daftar voter yang telah terdaftar			

Setelah melakukan pengujian terhadap cara kerja sistem ChainVote dalam melakukan voting diperoleh bahwa sistem berjalan dengan baik dan tidak memiliki *error*.

Responden yang sudah mencoba sistem ChainVote sebanyak 28 mahasiswa dari prodi diploma 3 Teknik Informatika angkatan 2016. Setiap responden melakukan voting untuk menentukan kualitas aplikasi.

Pengujian tersebut menghasilkan beberapa kesimpulan sebagai berikut :

1. Sistem berjalan dengan lancar.
2. Admin mendaftarkan voter dengan syarat email yang dimasukkan pada file excel daftar voter tidak boleh ada yang sama.

3. Setelah admin mendaftarkan voter maka sistem akan men-generate bitcoin address dan token masing-masing voter.
4. Voter dapat melakukan voting jika admin telah membayar bitcoin address yang telah terdaftar.
5. Voter tidak dapat melakukan voting jika status voting telah selesai.
6. Tidak ada satupun voter maupun admin yang mengetahui bitcoin address dan token yang ter-generate milik voter yang mana.
7. Token yang dipakai untuk melakukan voting hanya dapat digunakan sekali.
8. Apabila status voting telah berakhir maka token tidak dapat digunakan lagi.
9. Semua transaksi voting terhubung pada API SoChain.
10. Voter yang telah terdaftar pada sistem ChainVote hanya dapat memilih sekali.
11. Tidak ada satupun yang mengetahui hasil pilihan suara dari masing – masing voter, identitas voter yang memilih kandidat tersebut, identitas voter dari daftar token dan bitcoin address yang telah terdaftar.
12. Semua voter yang telah melakukan voting dapat melihat hasil voting dan dapat menghitung transaksi voting yang telah terdaftar.
13. Jika ada *user* yang memiliki hak akses masuk ke *database* maka user dapat memodifikasi nama kandidat yang terdaftar.
14. Sistem ChainVoting menggunakan server gmail untuk mengirimkan email kepada voter. Jadi jika ada user yang memiliki hak akses masuk ke server maka user dapat mengetahui token dikirimkan ke voter mana saja yang telah terdaftar.

Kendala yang dihadapi selama proses pengujian antara lain adalah koneksi internet yang tidak stabil dikarenakan untuk melakukan voting dan menghubungkan proses voting dengan API SoChain dibutuhkan koneksi internet yang stabil. Saat ini tempat peneliti dalam menjalankan proses pengujian aplikasi masih kurang koneksi internet sehingga responden yang melakukan pengujian pada sistem ChainVote sering mengalami kewalahan dalam melakukan voting.

BAB 7

HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan mengenai hasil dan pembahasan yang diperoleh setelah tahap implementasi dan pengujian Sistem E-voting menggunakan Teknologi Blockchain yang telah dibangun.

7.1 Hasil

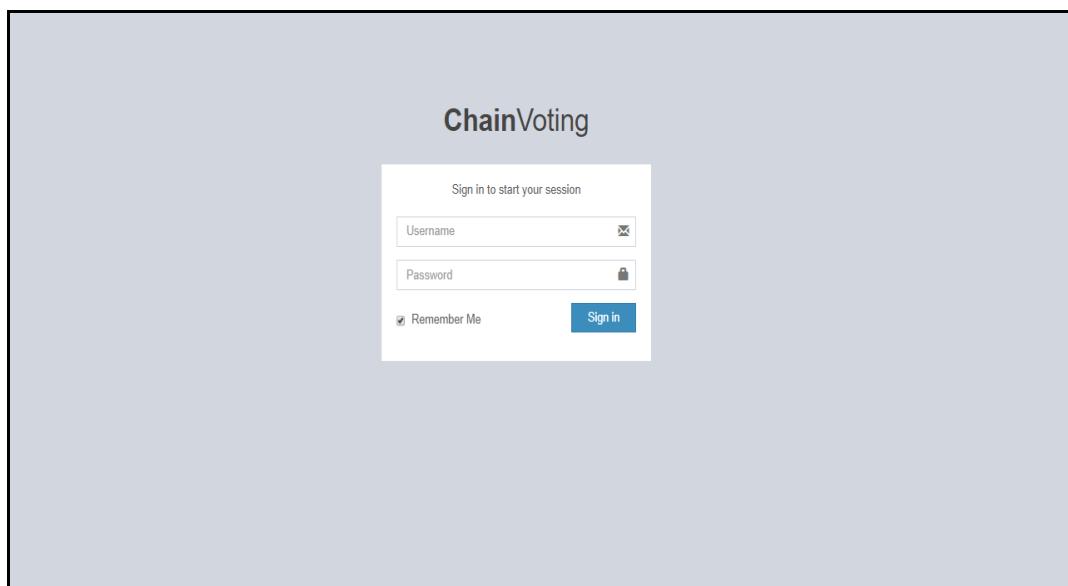
Pada sub bab ini dijelaskan bagaimana hasil aplikasi yang telah dibangun pada versi web. Adapun tampilan masing-masing fungsi dapat dilihat sebagai berikut.

7.1.1 Tampilan Sistem E-Voting menggunakan Teknologi Blockchain

Berikut tampilan aplikasi yang telah dibangun pada sistem e-voting.

1. Tampilan Login untuk Administrator

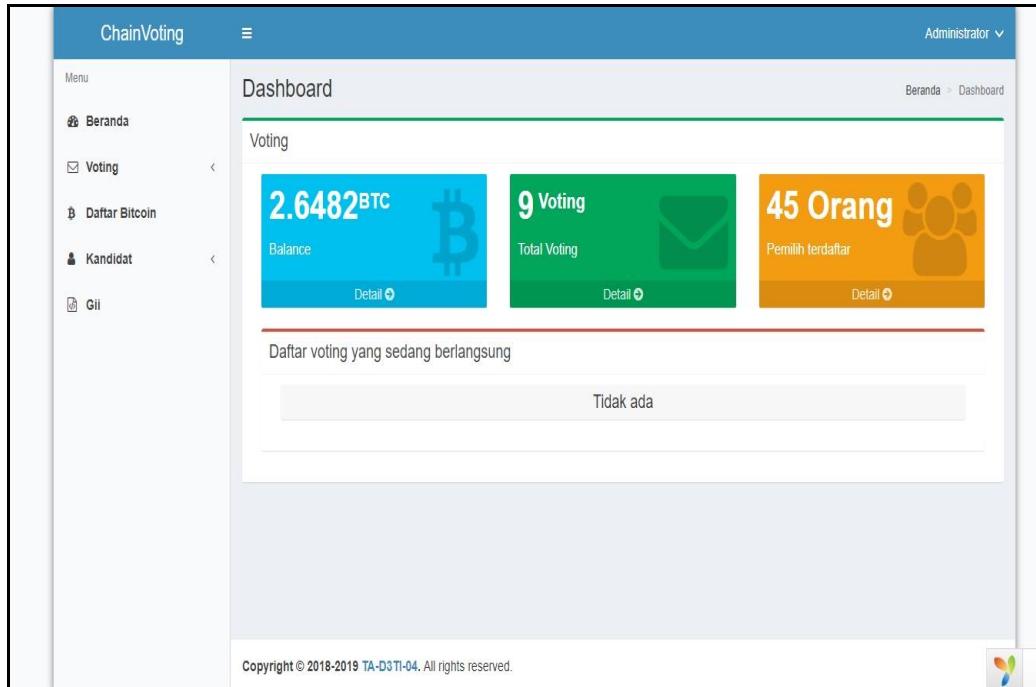
Tampilan dari halaman login untuk administrator pada sistem e-voting menggunakan teknologi blockchain dapat dilihat pada Gambar 7.1 berikut.



Gambar 7.1. Tampilan Login untuk Administrator

2. Tampilan Beranda

Tampilan dari halaman beranda pada sistem e-voting menggunakan teknologi blockchain dapat dilihat pada Gambar 7.2 berikut.



Gambar 7.2. Tampilan Beranda

Keterangan :

Tampilan halaman beranda merupakan tampilan awal sistem ChainVote setelah mengakses sistem ini. Pada halaman beranda menunjukkan balance (daftar transaksi dari layanan API SoChain yang telah terdaftar), daftar voting yang telah terdaftar, dan daftar bitcoin address yang telah digunakan dari daftar voter. Halaman beranda juga menampilkan menu-menu yang ada pada sistem ChainVote yaitu menu voting, menu daftar bitcoin, dan menu kandidat.

3. Tampilan Menambah Voting

Tampilan dari menambah voting pada sistem e-voting menggunakan teknologi blockchain oleh admin dapat dilihat pada Gambar 7.3 berikut.

The screenshot shows the 'Tambah Vote' (Add Voting) page of the ChainVoting application. The interface is in Indonesian. On the left, there's a sidebar with a 'Menu' section containing links for Voting, Daftar Voting, Tambah Voting, Daftar Bitcoin, Kandidat, and Gii. The main content area has a title 'Tambah Vote' and a breadcrumb navigation 'Beranda > Votes > Tambah Vote'. The form itself has several input fields: 'Nama Voting' (Name of Voting), 'Deskripsi' (Description) with a rich text editor, 'Tanggal Mulai' (Start Date) and 'Tanggal Berakhir' (End Date) with date pickers, a 'Kandidat' (Candidate) section with a 'Tambah Kandidat' (Add Candidate) button and a table for adding candidates (with columns for 'Nama Kandidat' (Candidate Name) and 'Deskripsi' (Description)), and a 'File Pemilih' (Voter File) section with a 'Browse...' button and a note about uploading an Excel file. At the bottom, there's a copyright notice 'Copyright © 2018-2019 TA-D3TI-04. All rights reserved.' and a logo.

Gambar 7.3. Tampilan Menambah Voting

Keterangan :

Tampilan menambah voting merupakan halaman untuk memasukkan data vote pada form tambah vote yang telah disediakan pada halaman ini. Pada halaman tambah vote tersedia form yang harus diisi admin untuk menambahkan daftar voting yaitu nama voting, deskripsi, tanggal mulai, tanggal berakhir, form untuk menambah kandidat yaitu nama kandidat dan deskripsi. Jika ingin menambah daftar kandidat lebih dari satu pilih menu tambah kandidat untuk menambah form tambah kandidat. Pada halaman ini juga tersedia form untuk memasukkan file daftar pemilih dalam bentuk excel. Tersedia tombol tambah untuk menambah dan menampilkan daftar voting.

4. Tampilan Daftar Voting

Tampilan dari daftar voting pada sistem e-voting menggunakan teknologi blockchain oleh admin dapat dilihat pada Gambar 7.4 berikut.

ChainVoting			
Administrator			
Menu	Voting		
Beranda Voting <ul style="list-style-type: none"> Daftar Voting Tambah Voting Daftar Bitcoin Kandidat GII			
	Nama Voting		
	<input type="button" value="Car"/>	<input type="button" value="Hapus"/>	
	Menampilkan 1-9 dari 9 item.		
#	Nama Voting	Deskripsi	Status
1	Ketua BEM 2016	ngetes	Selesai Rincian Hasil
2	Pemilihan mahasiswa berprestasi 2019	Pemilihhaann	Selesai Rincian Hasil
3	Mahasiswa cantik	testingg	Selesai Rincian Hasil
4	Ketua BEM 2016	ngetes	Selesai Rincian Hasil
5	Pemilihan ketua test	test	Sedang Mulai Rincian Hasil Sementara
6	Ketua HIMATIF	Pemilihan Ketua HIMATIF tahun 2019/2020. Siapakah yang layak menjadi Ketua HIMATIF?	Selesai Rincian Hasil
7	Pemilihan Kadep Pendidikan 2019	Untuk angkatan 2018	Selesai Rincian Hasil
8	beasiswa pintar	kamuuu terpilih	Selesai Rincian Hasil
9	Mahasiswa Teladan 2020	pemilihan ini untuk mahasiswa angkatan 2018	Sedang Mulai Rincian Hasil Sementara

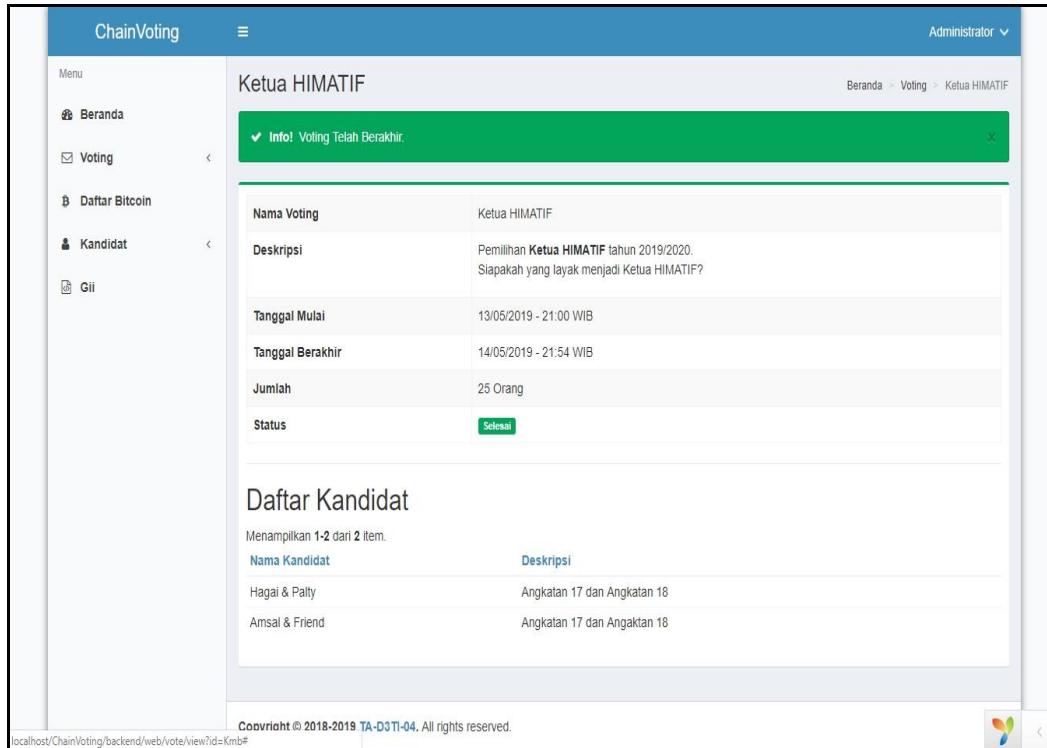
Gambar 7.4. Tampilan Daftar Voting

Keterangan :

Pada halaman daftar voting merupakan semua daftar voting yang telah didaftarkan oleh admin. Pada halaman ini menampilkan form nama voting untuk pencarian dan pemhapusan nama voting yang diinput pada form. Selain form nama voting, halaman ini menampilkan informasi masing – masing nama voting, deskripsi, status voting, menu rincian untuk melihat rincian daftar voting, dan menu hasil untuk melihat hasil voting.

5. Tampilan Rincian Daftar Voting

Tampilan dari rincian daftar voting pada sistem e-voting menggunakan teknologi blockchain oleh admin dapat dilihat pada Gambar 7.5 berikut.



Gambar 7.5. Tampilan Rincian Daftar Voting

Keterangan :

Halaman rincian voting merupakan halaman yang menampilkan rincian daftar voting yang menunjukkan informasi nama voting, deskripsi, tanggal mulai, tanggal berakhir, jumlah voting yang terdaftar, dan status voting saat ini. Selain menampilkan rincian daftar voting, halaman ini juga menampilkan daftar kandidat yang menunjukkan informasi masing – masing nama kandidat dan deskripsi kandidat.

6. Tampilan Membuat Daftar Kandidat

Tampilan dari membuat daftar kandidat pada sistem e-voting menggunakan teknologi blockchain oleh admin dapat dilihat pada Gambar 7.6 berikut.

The screenshot shows the 'Tambah Kandidat' (Add Candidate) page of the ChainVoting application. The left sidebar has a 'Menu' section with 'Voting' selected. Below it are 'Daftar Bitcoin', 'Kandidat' (with 'Daftar Kandidat' and 'Tambah Kandidat' sub-options), and 'Gii'. The main content area has a title 'Tambah Kandidat' and a breadcrumb 'Beranda > Candidates > Tambah Kandidat'. It contains three input fields: 'Nama Kandidat' (Candidate Name), 'Deskripsi' (Description) with a WYSIWYG editor toolbar, and a 'Voting' dropdown menu currently set to 'Pemilihan mahasiswa berprestasi 2019'. At the bottom is a green 'Save' button. The footer includes a copyright notice 'Copyright © 2018-2019 TA-D3TI-04. All rights reserved.' and a small logo.

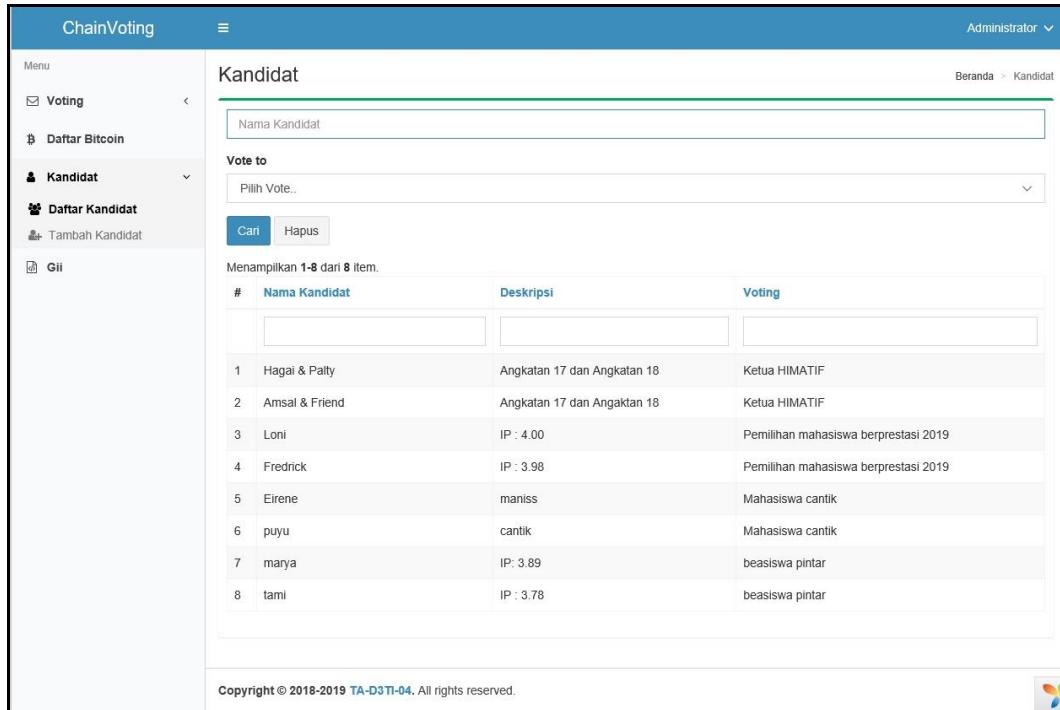
Gambar 7.6. Tampilan Membuat Daftar Kandidat

Keterangan :

Tampilan membuat daftar kandidat merupakan halaman untuk memasukkan data atau informasi mengenai kandidat pada form tambah kandidat yang telah disediakan pada halaman ini. Pada halaman tambah kandidat tersedia form yang harus diisi admin untuk menambahkan daftar kandidat yaitu nama kandidat, deskripsi, dan *drop down list* voting. Tersedia tombol *save* untuk menambah dan menampilkan daftar kandidat.

7. Tampilan Daftar Kandidat

Tampilan dari daftar kandidat pada sistem e-voting menggunakan teknologi blockchain oleh admin dapat dilihat pada Gambar 7.7 berikut.



Gambar 7.7. Tampilan Daftar Kandidat

Keterangan :

Pada halaman daftar kandidat merupakan semua daftar kandidat yang telah didaftarkan oleh admin. Pada halaman ini menampilkan form nama kandidat dan *drop down list vote to* untuk pencarian dan penghapusan nama kandidat dan vote to yang diinput pada form. Selain itu, halaman ini juga menampilkan informasi masing-masing nama kandidat, deskripsi, dan voting.

8. Tampilan Daftar Bitcoin Address

Tampilan dari daftar bitcoin address pada sistem e-voting menggunakan teknologi blockchain dapat dilihat pada Gambar 7.8 berikut.

#	Bitcoin Address	Status	Voting	Operasi
1	muqFUCLSyCmLh114z4hF8sBqY6AKTjntdE	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi
2	mg1Ntnk6SqYaknaFS4ga5RyVZHRQDGfCSkz	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi
3	mz1qYAxUHMGNXVmzKsBbBtQ1W3huia7bS	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi
4	myss6WGUHhocJGNkFWgFmJ9TDkGCrVSiN	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi
5	mwCifG48tGHUMQD9Zk4tns58wac3S37Cap	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi
6	mtorSE2WfyZo4VFDIJrgDhD8WWBjhKME	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi
7	mkZgXfj8VlkxUMAC9s1F8KHKEAMxoAzcUk	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi
8	n1mELxsmUwJDVP7yNPeQHxDcRa3BGJWL	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi
9	mrPc8eo7zkFGGz8K8bikuSgJHS84aLdjEj	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi
10	rnsJ2DTNEHvCnJuotmByJ9n4CwG6pfSxW54	Belum Aktif	Ketua dan Wakil Ketua HIMATIF	Aktivasi

Gambar 7.8. Tampilan Daftar Bitcoin Address

Keterangan :

Tampilan daftar bitcoin address merupakan halaman yang menampilkan daftar bitcoin address yang sudah digunakan dan belum digunakan. Pada halaman ini admin membayar bitcoin address yang belum digunakan. Untuk dapat melakukan voting admin harus membayar bitcoin address dari daftar voter yang telah terdaftar. Jika bitcoin address sudah digunakan maka akan masuk ke kolom yang sudah digunakan. Bitcoin address digunakan oleh voter untuk terhubung pada API SoChain agar dapat mengambil detail transaksi voting di blockchain.

9. Tampilan Daftar Voting untuk Voter

Tampilan dari daftar voting untuk voter pada sistem e-voting menggunakan teknologi blockchain dapat dilihat pada Gambar 7.9 berikut.

CHAINVOTING		DAFTAR VOTING			
Beranda / Daftar Voting					
Menampilkan 1-4 dari 4 item.					
#	Judul	Deskripsi	Status		
1	Pemilihan mahasiswa berprestasi 2019	Pemilihaaaann	Selesai Q. Hasil		
2	Mahasiswa cantik	testingg	Selesai Q. Hasil		
3	Ketua HIMATIF	Pemilihan Ketua HIMATIF tahun 2019/2020. Siapakah yang layak menjadi Ketua HIMATIF?	Selesai Q. Hasil		
4	beasiswa pintar	kamuuu terpilih	Selesai Q. Hasil		

Copyright © 2018-2019 TA-D3TI-04. All rights reserved.

Gambar 7.9. Tampilan Daftar Voting untuk Voter

Pada halaman daftar voting untuk voter merupakan semua daftar voting yang telah digunakan untuk melakukan voting. Halaman ini dapat dilihat oleh voter setelah melakukan voting. Pada halaman ini menampilkan informasi masing – masing nama voting, deskripsi, status voting apakah sudah selesai atau sedang berlangsung, dan menu hasil untuk melihat hasil voting.

10. Tampilan Email untuk Voting

Tampilan dari email untuk voting pada sistem e-voting menggunakan teknologi blockchain dapat dilihat pada Gambar 7.10 berikut.



Gambar 7.10. Tampilan Email untuk Voting

Keterangan :

Tampilan email untuk voting berisi link untuk melakukan voting dan alamat token. Email ini dikirim pada masing-masing voter yang telah terdaftar setelah admin mendaftarkan daftar voter pada sistem ChainVote.

11. Tampilan Form Memasukkan Token

Tampilan dari form memasukkan token untuk memulai voting pada sistem e-voting menggunakan teknologi blockchain dapat dilihat pada Gambar 7.11 berikut.

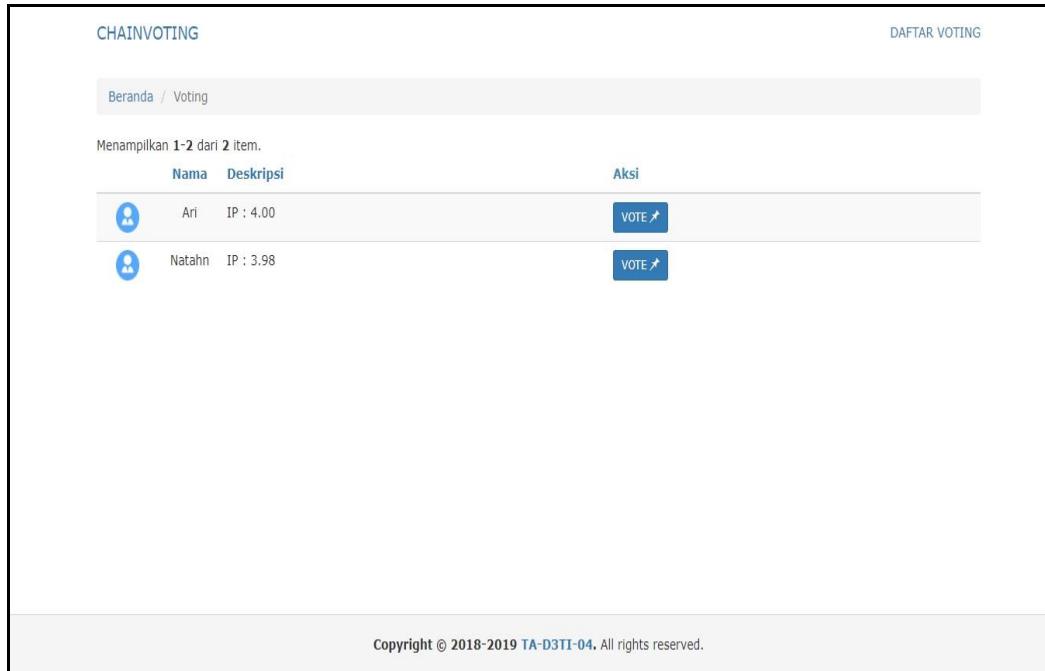
Gambar 7.11. Tampilan Form Memasukkan Token

Keterangan :

Tampilan form memasukkan token merupakan halaman yang digunakan voter untuk memasukkan alamat token. Untuk dapat melakukan voting, setiap voter yang telah terdaftar terlebih dahulu memasukkan alamat token pada halaman form token. Alamat token diperoleh dari email yang terkirim pada voter yang telah terdaftar. Email yang dikirim pada voter berisi alamat token dan link untuk melakukan voting. Token hanya dapat digunakan sekali untuk melakukan voting. Token yang sudah pernah digunakan tidak dapat dipakai lagi untuk melakukan voting.

12. Tampilan Daftar Voting Melakukan Vote

Tampilan dari daftar voting untuk melakukan vote pada sistem e-voting dapat dilihat pada Gambar 7.12 berikut.



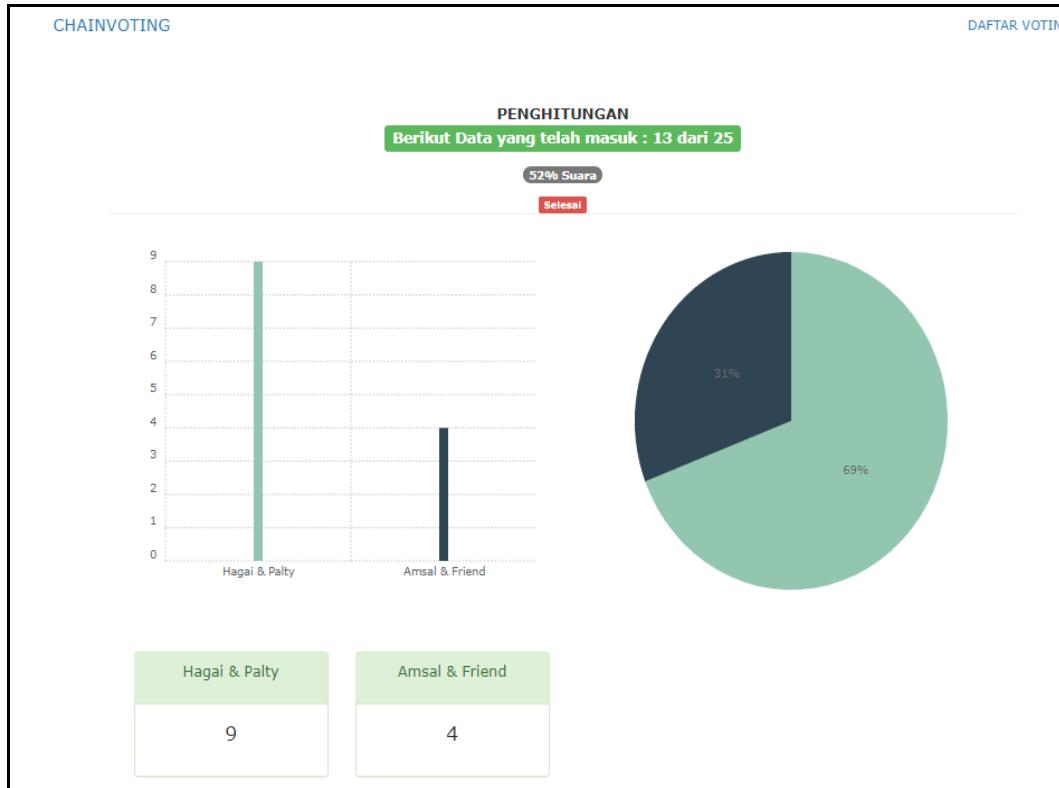
Gambar 7.12. Tampilan Daftar Voting untuk Melakukan Vote

Keterangan :

Tampilan daftar voting ini merupakan daftar voting yang dapat diakses oleh voter untuk melakukan voting. Untuk dapat mengakses halaman daftar vote, voter harus terlebih dahulu memasukkan alamat token yang valid pada halaman form token. Pada halaman daftar vote menampilkan informasi masing-masing nama kandidat, deskripsi, voting, dan tombol vote untuk melakukan voting.

13. Tampilan Hasil Voting

Tampilan dari hasil voting pada sistem e-voting dapat dilihat pada Gambar 7.13 berikut.



Gambar 7.13. Tampilan Hasil Voting

Keterangan :

Tampilan hasil voting merupakan halaman yang menampilkan detail hasil voting. Pada halaman ini menunjukkan data yang telah masuk (jumlah voter yang telah melakukan voting), jumlah voter yang telah terdaftar, diagram lingkaran yang menampilkan hasil voting masing-masing kandidat, dan hasil voting juga menampilkan jumlah voter yang memilih masing-masing kandidat (data vote yang masuk pada masing-masing kandidat).

14. Tampilan Halaman Voting Selesai

Tampilan dari halaman voting jika status voting telah berakhir pada sistem e-voting dapat dilihat pada Gambar 7.14 berikut.



Gambar 7.14. Tampilan Halaman Voting Selesai

Keterangan :

Pada halaman voting telah selesai untuk voter menampilkan voting telah selesai. Voting selesai jika waktu voting yang telah ditentukan oleh admin telah berakhir. Jadi jika waktu voting telah berakhir, voter tidak dapat lagi melakukan voting.

15. Tampilan Detail Transaksi Voting pada Blockchain

Tampilan dari detail transaksi voting pada blockchain dapat dilihat pada Gambar 7.15 berikut.

```
"outputs" : [
    {
        "output_no" : 0,
        "address" : "nulldata",
        "value" : "0.00000000",
        "type" : "nulldata",
        "req_sigs" : null,
        "spent" : null,
        "script_asm" : "OP_RETURN 766f74696e674b6d62303131",
        "script_hex" : "6a0c766f74696e674b6d62303131"
    },
]
```

Gambar 7.15. Tampilan Detail Transaksi Voting pada Blockchain

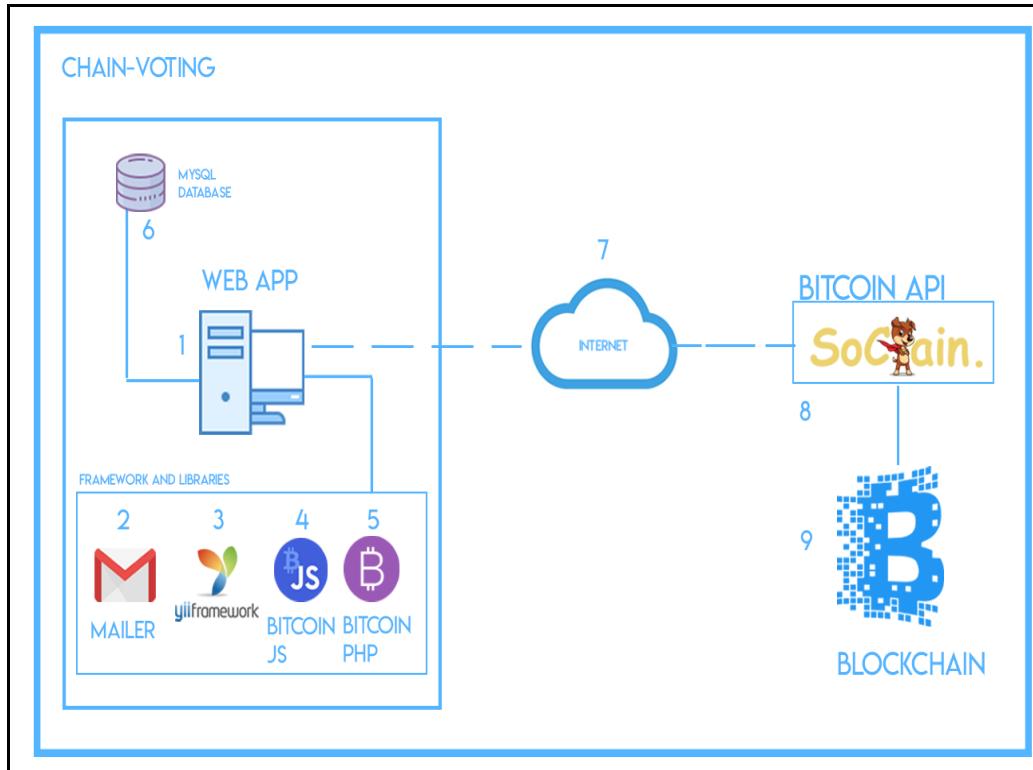
Keterangan :

Pada Gambar 7.15 detail transaksi voting bahwa outputs script menampilkan hasil transaksi voting pada “script_asm” yaitu OP_RETURN 766f7469e674b6d62303131. Untuk mendekode transaksi voting ke *plaintext* penulis menggunakan fungsi hex2bin untuk mengkonversi menjadi karakter. Dengan mengkonversi OP_RETURN penulis mendapatkan pesan “voting011007”. OP_RETURN digunakan menyimpan pesan transaksi voting. Dalam implementasi peneliti menggunakan OP_RETURN untuk menyimpan pesan transaksi voting.

7.2 Pembahasan

Sistem E-voting telah berhasil dibangun dengan menggunakan teknologi blockchain. Ada dua tujuan yang akan dicapai pada Tugas Akhir ini yang pertama adalah merancang dan membangun sistem e-voting dengan menggunakan teknologi blockchain dan kedua adalah membuktikan keamanan hasil data voting untuk mencapai aspek *accuracy*, *invulnerability*, *privacy*, dan *verifiability*.

Berdasarkan tahapan yang telah dilakukan peneliti berhasil merancang dan membangun sistem e-voting dengan menggunakan teknologi blockchain sesuai dengan tujuan tugas akhir pada poin pertama. Peneliti membuat arsitektur sistem e-voting menggunakan teknologi blockchain untuk menjelaskan sistem e-voting yang telah diimplementasikan. Berikut arsitektur sistem e-voting menggunakan teknologi blockchain ditunjukkan pada Gambar 7.16 berikut.



Gambar 7.16. Arsitektur Sistem E-Voting menggunakan Teknologi Blockchain

Keterangan arsitektur sistem e-voting menggunakan teknologi blockchain :

1. Merancang dan membangun Web APP sistem e-voting menggunakan teknologi blockchain berbasis web.
2. Sistem e-voting menggunakan *server* gmail untuk mengirimkan email kepada masing-masing voter yang telah didaftarkan pada sistem.
3. Web App sistem e-voting menggunakan teknologi blockchain dibangun menggunakan framework yii2, bahasa pemrograman PHP dan JavaScript.
4. Sistem e-voting yang dibangun menggunakan library Bitcoin JS. Library Bitcoin JS digunakan untuk melakukan transaksi pada API SoChain.
5. Sistem e-voting yang dibangun juga menggunakan library Bitcoin PHP. Library Bitcoin JS digunakan untuk untuk men-*generate* bitcoin address.
6. Untuk menyimpan data yang ada pada sistem e-voting menggunakan database MySQL.
7. Koneksi internet sangat dibutuhkan untuk menghubungkan Web App dengan API Blockchain.
8. Untuk menghubungkan web app dengan blockchain peneliti menggunakan salah satu API Blockchain yaitu layanan API SoChain. API SoChain

adalah layanan yang digunakan untuk membuat dan mengambil transaksi voting pada blockchain berdasarkan bitcoin address.

9. API SoChain merupakan salah satu API Blockchain yang umumnya digunakan untuk membuat transaksi yang terhubung dengan sistem lain.

Jadi dapat disimpulkan bahwa peneliti berhasil merancang dan membangun sistem e-voting menggunakan teknologi blockchain melalui implementasi yang telah dilakukan.

Setelah dilakukan pengujian pada sistem e-voting, maka dapat dibuktikan metode keamanan sistem e-voting menggunakan teknologi blockchain sudah tercapai sesuai tujuan tugas akhir pada point kedua. Berikut penjelasan bahwa sistem e-voting menggunakan teknologi blockchain sudah memenuhi aspek metode keamanan yang telah penulis tentukan.

1. Accuracy

Aspek ini menjelaskan bahwa suatu sistem akurat jika tidak mungkin hasil suara dapat dimodifikasi, tidak mungkin hasil vote yang divalidasi dihilangkan dari perhitungan akhir, dan tidak mungkin suara yang tidak sah untuk dihitung dalam perhitungan akhir.

Berikut penjelasan bahwa sistem ChainVote telah memenuhi aspek *accuracy*.

Setelah voter melakukan vote hasil voting akan dihubungkan dengan layanan API Blockchain. Dengan teknologi blockchain yang bersifat *immutable* atau tidak dapat diubah sehingga membuat data transaksi voting pada penyimpanan blockchain sulit dilakukan modifikasi. Setiap transaksi voting yang pernah terjadi dan telah terdaftar pada jaringan blockchain akan disimpan pada penyimpanan data atau blok yang terdistribusi. Jadi blok berisi transaksi voting yang terjadi pada waktu tertentu. Masing-masing blok memiliki fungsi hash yang digunakan untuk mengambil nilai hash dari data transaksi sebelumnya untuk menjadi input nilai hash pada blok berikutnya. Jadi setiap blok saling berhubungan dengan blok berikutnya. Blockchain juga bersifat terdistribusi yang berarti database transaksi blockchain tidak hanya disimpan pada satu server saja tetapi pada semua server yang terlibat dalam jaringan blockchain sehingga membuat setiap transaksi pada blok transparan. Hal inilah yang membuat data pada blockchain sulit dimodifikasi. Jadi jika ada seorang peretas yang ingin memodifikasi transaksi pada database

blockchain, seseorang tersebut harus mampu mengubah database transaksi sebelumnya dan sesudahnya yang menyimpan transaksi lainnya. Oleh karena itu teknologi blockchain memberikan tingkat keamanan yang tinggi khususnya mencegah modifikasi database blockchain. Namun untuk aspek *accuracy* pada sistem ini masih memiliki kelemahan yaitu daftar kandidat yang tersimpan pada *database* masih dapat diubah jika adanya user yang memiliki hak akses masuk ke server database voting.

2. Invulnerability

Aspek ini menjelaskan bahwa sistem hanya mengizinkan pemilih yang berhak untuk memilih dan memastikan bahwa masing-masing pemilih dapat memilih hanya sekali.

Berikut penjelasan bahwa sistem ChainVote telah memenuhi aspek *invulnerability*.

Pemilih yang berhak memilih pada sistem ChainVote adalah voter yang telah didaftarkan admin pada sistem dan mendapatkan email link untuk melakukan voting dan token untuk mengakses vote. Syarat yang harus dipenuhi supaya voter terdaftar pada sistem adalah email yang didaftarkan tidak boleh ada yang sama dengan voter lainnya. Setelah admin mendaftarkan voter maka akan sistem akan men-generate bitcoin address dan token setiap voter. Sebelum melakukan vote admin harus terlebih dahulu membayar bitcoin address dari setiap voter yang terdaftar. Token untuk vote akan dikirimkan melalui email kepada setiap voter. Token ini digunakan untuk mengakses halaman untuk melakukan voting. Jadi untuk memastikan bahwa masing-masing pemilih dapat memilih hanya sekali yaitu melalui token yang digunakan untuk melakukan voting. Token yang telah digunakan hanya dapat digunakan sekali melakukan voting dan token yang tidak terpakai tidak dapat digunakan jika status voting telah berakhir.

3. Privacy

Aspek ini menjelaskan bahwa suatu sistem e-voting bersifat *privacy* jika tidak ada otoritas pemilihan atau orang lain dapat menghubungkan surat suara apa pun dengan pemilih yang memberikannya, dan tidak ada pemilih yang dapat membuktikan bahwa ia memilih dengan cara tertentu serta tidak ada pemilih yang mengetahui hasil suara dari orang lain.

Berikut penjelasan bahwa sistem ChainVote telah memenuhi aspek *privacy*.

Pada sistem ChainVote data voting yang menjadi *privacy* adalah hasil suara masing-masing voter, identitas voter yang memilih kandidat tersebut, identitas voter dari masing-masing daftar token yang telah *digenerate*, dan token yang telah digunakan ataupun belum digunakan serta identitas dari voter yang memiliki token tersebut.

Namun sistem ini masih memiliki kelemahan pada aspek *privacy*. Dalam implementasi peneliti menggunakan sistem luar untuk melakukan proses vote yaitu server gmail untuk mengirimkan email kepada voter yang terdaftar pada sistem ChainVote. Jadi jika ada user yang memiliki hak akses pada *server* gmail, user tersebut akan mengetahui kepada siapa saja atau voter yang terkirim email untuk link voting dan alamat token untuk mengakses vote. Ini merupakan kelemahan aspek *privacy* data voting pada sistem.

4. Verifiability

Aspek ini menjelaskan bahwa suatu sistem e-voting bersifat *verifiability* jika ada yang secara independen dapat memverifikasi bahwa semua suara yang telah dihitung terkoreksi dengan benar.

Tahapan yang dilakukan untuk verifikasi dan perhitungan vote di blockchain adalah sebagai berikut :

1. Secara otomatis sistem mengambil semua transaksi voting berdasarkan bitcoin address pada API SoChain.
2. Sistem mengambil kode OP_RETURN hasil dari transaksi voting. Pesan yang akan diambil dari transaksi untuk dilakukan perhitungan adalah kode OP_RETURN hasil voting. Pesan ini akan diubah menjadi format hexadecimal.
3. Decode kode OP_RETURN menjadi id_kandidat dan id_vote.
4. Substring hasil voting untuk mengambil atau memotong sebagian nilai dari suatu string.
5. Verifikasi validitas setiap suara yang terpilih.
6. Sistem menghitung hasil voting yang valid dan sistem akan menambahkan satu suara ke kandidat yang terpilih akan bertambah.

Berikut penjelasan bahwa sistem ChainVote telah memenuhi aspek *verifiability*.

1. Untuk perhitungan data vote yang masuk

Untuk data vote yang masuk pada sistem diperoleh dengan data yang telah masuk (jumlah voter yang telah melakukan voting) dibagi dengan jumlah voter yang telah terdaftar pada sistem lalu hasilnya dikalikan dengan seratus persen, sehingga diperoleh perhitungan data vote yang masuk. Jumlah voter yang telah melakukan voting dan jumlah voter yang terdaftar dapat dibuktikan dengan melihat jumlah bitcoin address yang telah digunakan.

2. Hasil voting masing-masing kandidat

Hasil voting masing-masing kandidat diperoleh dengan jumlah voter yang memilih kandidat dibagi dengan jumlah data vote yang masuk (jumlah voter yang telah melakukan voting) lalu hasilnya dikalikan dengan seratus persen, sehingga diperoleh hasil voting masing-masing kandidat.

3. Jumlah voter yang memilih masing-masing kandidat

Jumlah voter yang memilih masing-masing kandidat diperoleh sesuai dengan jumlah suara yang masuk (data vote yang masuk) untuk masing-masing kandidat pada sistem ChainVote.

Jadi dapat disimpulkan bahwa sistem ChainVote telah memenuhi aspek *verifiability* karena sistem ChainVote dapat memverifikasi bahwa semua suara yang telah dihitung terkoreksi dengan benar sesuai hasil perhitungan yang telah dilakukan.

Setelah melalui tahapan dimulai dari menentukan topik, perumusan masalah, studi pustaka, analisis, design, implementasi, dan pengujian dapat disimpulkan bahwa penulis berhasil mencapai tujuan Tugas Akhir ini yaitu yang pertama adalah merancang dan membangun sistem e-voting dengan menggunakan teknologi blockchain dan kedua adalah membuktikan keamanan hasil data voting untuk mencapai aspek *accuracy*, *invulnerability*, *privacy*, dan *verifiability*.

7.3 Kendala

Pembangunan Sistem E-Voting menggunakan Teknologi Blockchain dalam pengerjaan Tugas Akhir ini tidak terlepas dari kendala yang dihadapi. Berikut beberapa kendala yang dihadapi pada pengerjaan Tugas Akhir ini yaitu :

1. Bitcoin Tesnet

- a) Untuk melakukan voting, bitcoin address harus dibayar terlebih dahulu. Oleh sebab itu, admin harus memiliki bitcoin tesnet untuk

melakukan pembayaran untuk mendapatkan bitcoin tesnet sejumlah 0.001 BTC. Pembayaran ini membutuhkan waktu dan jumlah ini digunakan untuk satu voter saja. Hal inilah yang menyebabkan proses voting terkendala.

- b) Apabila seseorang mengetahui bitcoin address voting, OP_RETURN untuk voting dan cara broadcast transaksi maka memungkinkan untuk melakukan voting di luar sistem sehingga hal ini menyebabkan data yang masuk tidak valid.

2. Database

Untuk database daftar kandidat belum menggunakan blockchain. Sehingga menyebabkan daftar kandidat pada database masih dapat diubah oleh pihak tertentu yang memiliki hak akses masuk ke server database.

BAB 8

KESIMPULAN DAN SARAN

Pada bab ini dijelaskan mengenai kesimpulan dari Tugas Akhir yang sudah dilakukan berdasarkan hasil pembahasan yang telah disampaikan dan saran–saran untuk pengembangan sistem selanjutnya.

8.1 Kesimpulan

Adapun kesimpulan yang diperoleh selama penggeraan Tugas Akhir ini, yaitu sebagai berikut :

1. Sistem yang dibangun telah menghasilkan sistem e-voting menggunakan teknologi blockchain berbasis web.
2. Sistem E-Voting menggunakan Teknologi Blockchain telah memenuhi aspek keamanan meliputi *accuracy*, *invulnerability*, *privacy*, dan *verifiability*. Namun untuk aspek *accuracy* masih memiliki kelemahan yaitu daftar kandidat yang terdaftar pada *database* masih dapat diubah jika user memiliki hak akses ke database. dan untuk aspek *privacy* pada sistem juga masih memiliki kelemahan dikarenakan sistem ChainVoting menggunakan sistem luar yaitu server gmail sehingga kemungkinan besar seseorang yang memiliki hak akses ke server dapat mengetahui token dikirimkan ke voter mana saja yang telah terdaftar.
3. Blockchain belum solusi untuk kerahasiaan negara untuk pemilihan umum.

8.2 Saran

1. Pada penelitian selanjutnya peneliti diharapkan dapat mengintegrasikan semua data voting dari database ke Blockchain untuk menghindari pengubahan data pada voting dan untuk Bitcoin Testnet sebaiknya menggunakan Bitcoin Testnet Virtual sendiri sehingga mempermudah pengisian Bitcoinnya.
2. Pada penelitian selanjutnya peneliti diharapkan untuk menerapkan digital signature untuk melakukan voting sehingga vote (voting_id, candidat_id) yang dikirimkan lebih terjaga kerahasiaannya dan meminimalisir kemungkinan seseorang melakukan kegiatan voting diluar sistem.

3. Pada penelitian selanjutnya peneliti diharapkan peneliti dapat mengintegrasikan sistem ini dengan polling di CIS (*Campus Information System*) di IT Del.

DAFTAR PUSTAKA

- [1] Risnanto, S. (2017). Aplikasi Pemungutan Suara Elektronik/E-Voting Menggunakan Teknologi Short Message Service Dan At Command.
- [2] Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman Vignesh. (n.d.). Blockchain Technology. *Sutardja Center for Entrepreneurship & Technology Barkeley Engineering*.
- [3] Setiowati, D. A., R, B. M., & Jati, R.H. (2017). Pemograman Framework. Universitas Pembangunan Nasional “Veteran” Jawa Timur.
- [4] Kovic, M. (2017). *Blockchain for the people*. ZIPAR-Zurich Institute of Public Affairs Research.
- [5] Rokhman, A. (2011). Prospek dan Tantangan Penerapan e-Voting di Indonesia. Seminar Nasional Peran Negara dan Masyarakat dalam Pembangunan Demokrasi dan Masyarakat Madani di Indonesia Universitas Terbuka, Jakarta.
- [6] Risnanto, S. (2013, Desember). Merubah Sistem Pemilihan Kepala Daerah Dari Konvensional ke Digital (E-Pilkada). *ISU TEKNOLOGI STT MANDALA*, 6, 103-106.
- [7] Isnaini , M. F. (2009). Analisis Dan Implementasi E-Voting System Pada Pemilihan Kepala Daerah. Fakultas Matematika dan Ilmu Pengetahuan Alam Institut Pertanian Bogor, Bogor.
- [8] Policy Paper. 2011. *Introducing Electronic Voting Essential Considerations*. International IDEA. Stockholm.
- [9] Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman Vignesh. (n.d.). Blockchain Technology. *Sutardja Center for Entrepreneurship & Technology Barkeley Engineering*. (3)
- [10] Setiowati, D. A., R, B. M., & Jati, R.H. (2017). Pemograman Framework. Universitas Pembangunan Nasional “Veteran” Jawa Timur. (4)
- [11] Barnes, A., Brake, C., & Perry, T. (n.d.). Digital Voting with the use of Blockchain Technology. *Team Plymouth Pioneers-Plymout University*.
- [12] Rahardjo, B. (2005). Keamanan Sistem Informasi Berbasis Internet. Bandung : PT. Insan Indonesia.
- [13] Cranor, L. F., & Cytron, R. K. (1997). Sensus : A Security-Conscious Electronic Polling Sytem for the Internet. *Proceedings of The Annual Hawwai International Conference*.
- [14] Hasibuan, Z. A., & Kurniawan, H. (n.d.). Pengembangan Protokol Routing Untuk Menjamin Kualitas Perpustakaan Digital Berbasis Peer to Peer. Ilmu Komputer dan Informasi, 2.
- [15] Wijaya, A. B., Soeprapto, J., & Tegar, Y. (2015). Analisis Arsitektur Perancangan Sistem Terdistribusi Menggunakan Model Nested Transaction pada Lingkungan Kerja Perkantoran. *Majalah Ilmiah*, 07.s

- [16] Dharmasurya, A., Wahyono, T., & Somnya, R. (2013). Pengembangan Sistem Terdistribusi untuk Sistem Informasi Administrasi Kependudukan dengan Integrasi Teknologi RMI dan Web Service. *Jurnal Teknologi Informasi-Aiti*, 10.
- [17] W, M. H. (2009). Perkembangan Enkripsi Fungsi Hash pada SHA (Secure Hash Algorithm). Institut Teknologi Bandung.
- [18] V, S. (n.d.). *On Fast and Provably Secure Message Authentication Based on Universal Hashing Advances in Cryptology*. CRYPTO, LNCS. 1109, 313-328.
- [19] Ginting, A. C. (2017). Perbandingan Algoritma Message Digest 5 (MD5) dan SHA256 Pada Hashing File Dokumen. Universitas Sumatera Utara. Diperoleh dari <http://repository.usu.ac.id>
- [20] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.
- [21] Kurniawan, F., Kusyanti, A., & Nurwasito, H. (2017, Juni 9). Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 1, 803-812.
- [22] Sebastian, A. (2007). Implementasi dan Perbandingan Performa Algoritma Hash SHA-1, SHA-256, dan SHA 512. Institut Teknologi Bandung.
- [23] Syafriadi, M. (2006). Analisis Kecepatan dan Keamanan Algoritma Secure Hash Algorithm 256 (SHA-256) Untuk Otentikasi Pesan Teks. Institut Pertanian Bogor.
- [24] Rodiah, & Rahman, H. R. (2013). Otentikasi File dengan Algoritma Kriptografi SHA-1 Menggunakan Phyton dan Pycrypto. Universitas Gunadarma.
- [25] Lee, K., James, J., Ejeta, T., & Kim, H. (2016). *Electronic Voting Service Using Block-Chain*. *The Journal of Digital Forensics, Security and Law : JDFSL*, 11, 123.
- [26] Iyengar, S., Ramani, S.K, & Ao, B. (2018, November 26). *Fusion of the Brooks-Iyenger Algorithm and Blockchain in Decentralization of the Data-Source*. *Journal of Sensor and Actuator Networks*, 8,17.
- [27] Murach, J., & Harris, R. (2014). PHP and MySQL. United States of America: Mike Murach & Associate,Inc.
- [28] Prasetyo, D. D. (2003). Administrasi Database Server MySQL. Jakarta: PT Elex Media Komputindo.
- [29] Kurniawan, Y. (2002). Aplikasi Web Database dengan PHP dan MySQL. Jakarta: PT Elex Media Komputindo.
- [30] Shiran, Y., & Tomer. (1998). *Advanced JAVASCRIPT Programming*. New Delhi: Pressworks, Delhi.
- [31] Ramadhani, M. F. (2016). Pembangunan Aplikasi Informasi, Pengaduan, Kritik, dan Saran Seputar Kota Cimahi Pada Platform Android. *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*.

LAMPIRAN

Lampiran 1- Source Code Sistem

Pada Lampiran 1 ini akan diuraikan *source code* Sistem E-voting Menggunakan Teknologi Blockchain.

Source Code Sistem

Pada bagian ini ditampilkan *source code* pada setiap fungsi pada sistem e-voting menggunakan teknologi blockchain.

```
public function sendMail($email){  
    return Yii::$app->mailer->compose()  
        ->setTo($email)  
        ->setFrom([Yii::$app->params['adminEmail'] => 'Admin Voting'])  
        ->setSubject($this->subject)  
        ->setHtmlBody($this->body)  
        ->send();  
}
```

Lampiran 1. Source Code Fungsi untuk mengirim email ke voter

```
public function generateToken($n, $vote_id)  
{  
    $model = new Token();  
    $number = intval($n);  
    $bitcoin = new BitcoinECDSA();  
    $bitcoin->setNetworkPrefix('6f');  
    if ($n > 0 && $number < 1000) {  
  
        for ($i = 0; $i < $n; $i++) {  
            $token = $model->randomToken();  
            $model->token = $token;  
            $model->vote_id = $vote_id;  
            $bitcoin->generateRandomPrivateKey();  
        }  
    }  
}
```

```

$model->bitcoin_pubkey = $bitcoin->getPubKey();
$model->bitcoin_pvkey = $bitcoin->getWif();
$model->bitcoin_address = $bitcoin->getAddress();
if ($model->save(false)) {

    return $model->token;

}

}

return false;
}

```

Lampiran 2. Source Code Fungsi untuk mengenerate Token dan BitcoinAddress untuk Voter

```

$.getJSON("https://chain.so/api/v2/get_tx_unspent/BTCTEST/" + bitcoinAddress,
function(resultBtc){

    let last = resultBtc.data.txs.length - 1;
    let unspent_txid = resultBtc.data.txs[last].txid;
    let unspent_vout = resultBtc.data.txs[last].output_no;
    txb = new Bitcoin.TransactionBuilder(network);
    txb.addInput(unspent_txid,unspent_vout);
    let commit = new Buffered(Sha256.hash(pub_key));
    let dataScript = Bitcoin.script.nullData.output.encode(commit);
    value = Number(resultBtc.data.txs[last].value * 100000000);
    pay = 0.0001 * 100000000;
    change = parseInt(value - pay);
    console.log(change);
    txb.addOutput(dataScript,0);
    txb.addOutput(address,change);
}

```

```
txb.sign(0,keyPair);

var txRaw = txb.build();

var txHex = txRaw.toHex();

postdata = {tx_hex: txHex};

postValidation(id,postdata);

});

function postValidation(itemId,postdata){

$.post("https://chain.so/api/v2/send_tx/BTCTEST/",postdata,function (result) {

    if(result.status === "success"){

        $.getJSON("http://localhost/ChainVoting/backend/web/api/token/paid?i

d="+itemId,function () {

            if(result.status==="success"){

                document.location.reload(true);

            }

        });

    }

});
```

Lampiran 3. Source Code Fungsi untuk melakukan pembayaran ke voter agar voter dapat melakukan voting

```
$('.voteBtn').click(function(){
    var candidateId = $(this).attr('value');
    $.getJSON("/ChainVoting/backend/web/api/token/private?
tkn="+token,function (result) {
        wif = result.content.bitcoin_pvkey;
        network = Bitcoin.networks.testnet;
        keyPair = Bitcoin.ECPair.fromWIF(wif,network);
        var bitcoinAddress = keyPair.getAddress();
    });
});
```



```

    });
    });
    });
    });
}

```

Lampiran 4. Source Code Fungsi untuk melakukan pemilihan (Voter melakukan Voting)

```

function hex2bin (s) {
    var ret = [];
    var i = 0;
    var l;
    s += " ";
    for (l = s.length; i < l; i += 2) {
        var c = parseInt(s.substr(i, 1), 16);
        var k = parseInt(s.substr(i + 1, 1), 16);
        if (isNaN(c) || isNaN(k)) return false;
        ret.push((c << 4) | k);
    }
    return String.fromCharCode.apply(String, ret);
}

```

Lampiran 5. Source Code Fungsi hex2bin untuk mengkonversi OP_Return (hexadecimal menjadi biner (character))

```

function tallyingVoting(){
    admaddress = $('.admaddress').val();
    totalVoters = $('.vtnumbers').val();
    count = 0;
    $.getJSON(https://testnetapi.smartbit.com.au/v1/blockchain/address/
        +admaddress+"?limit=1000", function (result) {

```

```

if (result.success === true && result.address.total.transaction_count >0) {
    var item = result.address.transactions;
    for(var i=0; i<item.length;i++){
        (function(i){
            setTimeout(function(){
                if(i === item.length - 1 ){
                    $('#LoadingImage').hide();
                }else{
                    /** - */
                }
                counting(item[i].outputs[0].script_pub_key.hex);
            },i*200);
        })(i);
    }
}

else{
    $('#LoadingImage').hide();
    $(".tally-status").html('Data Belum Masuk')
        .addClass('label label-danger');
    $(".percentage").html('0%').addClass('badge');
}
}

function counting(hex){
    var item = hex2bin(hex);
    var voteId = item.substring(8,11);
    var candidateId = Number(item.substring(12,item.length));
    if( voteId === data.vote_id){
        for(var i = 0;i<data.id.length;i++){
            if(Number(data.id[i]) === candidateId){

```

```
    data.series[i] +=1;
    barData.series[i]+=1;
    count++;
}
}
}
}
```

Lampiran 6. Source code untuk proses penghitungan suara

Lampiran 2 – Langkah Menginstal Sistem E-Voting menggunakan Blockchain

Pada Lampiran 2 ini akan diuraikan cara menginstal Sistem E-voting Menggunakan Teknologi Blockchain.

Dapat diakses melalui link project ChainVoting
<https://bitbucket.org/marchelhutagalung/chainvoting/src/master/>

```

README.md

Cara Install

Tools yang harus dimiliki
• Git https://git-scm.com/download/win
• Composer https://getcomposer.org/download/

"NOTE: Lakukan semua perintah dalam command line dan berada pada root folder project"

Clone project ini ke folder project dengan perintah :
> git clone https://marchelhutagalung@bitbucket.org/marchelhutagalung/chainvoting.git

Update composer untuk menginstall dependency dengan perintah :
> composer update

Selanjutnya inisialisasi proyek ke development
> php init

Setelah itu akan muncul pesan
Which environment do you want the application to be initialized in?
[0] Development <br>
[1] Production

Pilih 0 untuk development. Lalu yes

```

Konfigurasi Database

Buka text editor anda, dan edit file `main-local.php` pada path `/common/config`

```

'components' => [
    'db' => [
        'class' => 'yii\db\Connection',
        'dsn' => 'mysql:host=localhost;dbname=chainvoting', //pastikan anda sudah membuat database dengan nama chainvoting
        'username' => 'root', //sesuaikan dengan username db anda
        'password' => '', //sesuaikan dengan password db anda
        'charset' => 'utf8',
    ],
],

```

Simpan configurasi tersebut lalu import `.sql` dump berikut ke database anda
<https://bitbucket.org/marchelhutagalung/chainvoting/downloads/chainvotingdb.sql>

Konfigurasi Host Email

Buka text editor anda, dan edit file `main-local.php` pada path `/common/config` dengan menambahkan code berikut pada Components

```

'mailer' => [
    'class' => 'yiisoft\swiftmailer\Mailer',
    'transport' => [
        'class' => 'Swift_SmtpTransport',
        'host' => 'smtp.gmail.com',
        'username' => '', // email gmail anda
        'password' => '', // password gmail anda
        'port' => '465',
        'encryption' => 'ssl',
    ],
],

```

USER

Username : administrator
Password : adminchainvoting2019

BITCOIN TESTNET

- Bitcoin Address : `moU5rEGoGaTXSPWjBKWMC68aLCbz7TQr6a`
- Untuk pengisian Bitcoin dapat menggunakan link berikut :

<https://tbtc.bitaps.com/>

Cara Akses

- Admin : <http://localhost/chainvoting/backend/web>
- Voter : <http://localhost/chainvoting/frontend/web>

Lampiran 7. Cara Menginstal Sistem E-Voting menggunakan Teknologi Blockchain