

IMPLEMENTASI TEKNOLOGI *BLOCKCHAIN* MENGUNAKAN *SMART CONTRACT* PADA *E-VOTING*

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik
Pada Jurusan Teknik Informatika

Oleh:

MUHAMMAD ZAKIE

11751100101



FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU

PEKANBARU

2021

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR PERSETUJUAN**IMPLEMENTASI TEKNOLOGI *BLOCKCHAIN*
MENGUNAKAN *SMART CONTRACT* PADA *E-VOTING*****TUGAS AKHIR**

Oleh

MUHAMMAD ZAKIE**11751100101**

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 24 Juni 2021

Pembimbing,

**NAZRUDDIN SAFAAT H., M.T.****NIP. 130 517 100**

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR PENGESAHAN

IMPLEMENTASI TEKNOLOGI *BLOCKCHAIN* MENGUNAKAN *SMART CONTRACT* PADA *E-VOTING*

TUGAS AKHIR

Oleh

MUHAMMAD ZAKIE

11751100101

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Informatika
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 24 Juni 2021

Pekanbaru, 24 Juni 2021

Mengesahkan,
Ketua Jurusan,

Dr. Elin Haerani, S.T., M.Kom.


NIP. 19810523 200710 2 003



Dr. Hartono, M.Pd.
NIP. 19640301 199203 1 003

DEWAN PENGUJI

Ketua : Jasril, S.Si, M.Sc
Sekretaris : Nazruddin Safaat H., M.T.
Penguji 1 : Novriyanto, S.T., M.Sc.
Penguji 2 : Muhammad Affandes, M.T.





LEMBAR HAK KEKAYAAN INTELEKTUAL

Tugas akhir yang tidak diterbitkan ini terdaftar dan tersedia di perpustakaan universitas islam negeri sultan syarif kasim riau adalah terbuka untuk umum dengan ketentuan bahwa hak cipta pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan seizin penulis dan harus disertai dengan kebiasaan ilmiah untuk menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh tugas akhir ini harus memperoleh izin dari dekan fakultas sains dan teknologi universitas islam negeri sultan syarif kasim riau. Perpustakaan yang meminjamkan tugas akhir ini untuk anggotanya diharapkan untuk mengisi nama, tanda peminjaman dan tanggal peminjaman.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



LEMBAR PERNYATAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan pada suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali secara tertulis terdapat dalam naskah ini dan disebutkan didalam daftar pustaka.

Pekanbaru, 24 Juni 2021

Yang membuat pernyataan,

MUHAMMAD ZAKIE

11751100101

UIN SUSKA RIAU

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Alhamdulillah Rabbil'alamin. Segala Puji bagi engkau Yaa Allah, Rabb semesta alam. Puji Syukur ku ucapkan kepada Allah Subhanahu waTa'ala, atas berkat dan pertolongan dari-Nya diri ini dapat menyelesaikan kewajiban terakhir di dunia perkuliahan, yakni laporan tugas akhir. Sungguh nikmat yang tak terkira dari engkau Yaa Allah, yang telah memberikan kesempatan bagi diri ini untuk bisa menyelesaikan laporan tugas akhir.

Laporan tugas akhir ini kupersembahkan untuk orang tua tercinta. Berkat kerja keras dan keringat beserta doa yang selalu orang tua berikan, sehingga diriku dapat menyelesaikan tugas akhir ini.

Tak lupa juga untuk seluruh teman-teman TIF F'17 dan teman-teman seperjuangan Teknik Informatika angkatan 17 yang telah bersedia membantu dan mendukung diri ini selama perkuliahan. Semoga Allah membalas tiap amal kebaikan yang telah kalian berikan dan Allah memberikan kesuksesan untuk kita nantinya setelah menyelesaikan perkuliahan di Teknik Informatika. AmiinnyaaRabbal'alamin.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

IMPLEMENTASI TEKNOLOGI *BLOCKCHAIN* MENGUNAKAN *SMART CONTRACT* PADA *E-VOTING*

MUHAMMAD ZAKIE

11751100101

Jurusan Teknik Informatika

Fakultas Sains dan Teknologi

Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

Teknologi saat ini berkembang sangat pesat dan sudah banyak manfaat dari penggunaan teknologi tersebut. Dengan adanya teknologi, seharusnya akan memudahkan dalam melakukan sistem voting di Indonesia dan mengatasi masalah pada sistem voting secara konvensional yang mana sistem tersebut menghabiskan biaya yang banyak dalam pelaksanaannya mulai dari pendataan pemilih sampai rekap hasil akhir dari perhitungan suara. Selain itu, juga mengatasi pemilih yang melakukan pemilihan dua kali lebih atau pemilih yang yang tidak memenuhi syarat dalam memilih, juga mengatasi kecurangan seperti membobol kotak suara. Walaupun begitu, bukan berarti sistem teknologi voting atau disebut juga dengan *e-voting* aman 100%, karena masih banyak celah keamanan pada sistem *e-voting* untuk bisa dibobol. Untuk itu keamanan dari *e-voting* harus ditambah dengan teknologi *blockchain* yang sangat aman karena menggunakan *hash sha-256* yang mana belum ada orang yang mampu memecahkan algoritma *sha-256* tersebut dan ditambah lagi bahwa *blockchain* berbentuk blok yang saling terhubung yang berada di jaringan *blockchain* secara *peer to peer* sehingga setiap transaksi ke *blockchain* akan divalidasi ke semua jaringan. Maka digunakanlah bahasa *solidity* yang merupakan cara untuk bisa menerapkan *smart contract* di *blockchain ethereum*.

Kata Kunci: *e-voting, blockchain, ethereum, solidity, smart contract*

- Hak Cipta Dilindungi Undang-Undang**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY USING SMART CONTRACT IN E-VOTING

MUHAMMAD ZAKIE

11751100101

Informatics Engineering

Faculty of Science and Technology

State Islamic University of Sultan Syarif Kasim Riau

ABSTRACK

Now technology is currently developing very fastly and there have been many benefits from using technology. With the existence of technology, it should make it easier to carry out a voting system in Indonesia and solve problems with the conventional voting system, where the system costs a lot of money in its implementation, from voter data collection to recapitulation of the final results of vote counting. Other than that, it also deals with voters who have made two more elections or those who do not meet the requirements to vote, as well as overcoming fraud such as breaking into ballot boxes. Even though, it does not mean that the voting technology system or also known as e-voting is 100% safe, because there are still many security holes in the e-voting system to be broken. Look at that, the security of e-voting must be added with blockchain technology which is very secure because blockchain uses sha-256 hash which no one has been able to solve the sha-256 algorithm and plus that the blockchain is in the form of interconnected blocks on the blockchain network. peer to peer so every transaction to the blockchain will be validated to all networks. So the solidity language is used which is a way to be able to implement smart contracts on the ethereum blockchain.

Kata Kunci: *e-voting, blockchain, ethereum, solidity, smart contract*

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalamu'alaikum wa rahmatullahi wa barakatuh

Alhamdulillah rabbil 'alamin, segala puji dan syukur bagi Allah 'Azza Wa Jalla yang senantiasa melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penelitian dan penulisan tugas akhir yang berjudul "Implementasi Teknologi *Blockchain* Menggunakan *Smart Contract* Pada E-Voting". Shalawat dan salam tidak lupa kita ucapkan kepada nabi Muhammad Shallallahu 'Alaihi Wa Sallam, yang telah mengubah dunia dari zaman yang penuh kesyirikan menuju zaman yang lurus dan sesuai tuntunan beserta ridha Allah 'Azza Wa Jalla, sehingga kita bisa berjalan di jalan yang lurus sesuai jalannya Rasulullah Shallallahu 'Alaihi Wa Sallam dan para sahabatnya yang telah di rihdoi-Nya.

Laporan tugas akhir ini disusun sebagai salah satu persyaratan untuk menyelesaikan Pendidikan Strata I (S1) Teknik Informatika pada Fakultas Sains dan Teknologi pada Universitas Islam Negeri Sultan Syarif Kasim Riau. Penulis sebagai manusia yang tidak luput dari kesalahan dan lupa, di dalam tugas akhir ini pun tidak lepas dari berbagai kekurangan, baik yang menyangkut teknis penyusunan, tata bahasa maupun isinya. Selama penulisan tugas akhir ini, penulis banyak mendapatkan pengetahuan, pengalaman, bimbingan, dukungan serta arahan dari semua pihak yang telah membantu dalam penulisan laporan tugas akhir ini baik secara langsung maupun tidak langsung sehingga dapat terselesaikan.

Untuk itu, pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Khairunnas, M. Ag selaku Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Bapak Dr. Hartono, M. Pd selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

3. Ibu Dr. Elin Haerani, S.T, M. Kom selaku Ketua Jurusan Teknik Informatika Universitas Islam Negeri Sultan Syarif Kasim Riau.
4. Bapak Iwan Iskandar, M.T., selaku Dosen Pembimbing Akademik yang telah memberikan nasehat selama perkuliahan.
5. Bapak Nazruddin Safaat H., M.T., selaku pembimbing I. terima kasih banyak telah memberikan ilmu, segala arahan, dorongan, motivasi dan bimbingan kepada penulis, serta selalu sabar menghadapi penulis dalam proses untuk menyelesaikan tugas akhir ini.
6. Bapak Novriyanto, S.T., M. Kom selaku penguji I. terima kasih untuk waktu, saran dan arahan yang telah diberikan sehingga laporan tugas akhir ini dapat diselesaikan.
7. Bapak Muhammad Affandes, M.T., selaku penguji II. Terima kasih untuk waktu, saran dan arahan yang telah diberikan sehingga laporan tugas akhir ini dapat diselesaikan.
8. Ibu Fitri Insani, S.T., M. Kom selaku penasehat akademik.
9. Seluruh Dosen Teknik Informatika yang telah memberikan ilmu dan bimbingan yang bermanfaat untuk kami.
10. Untuk kedua orang tua tercinta, Ayahanda Khairul Amri dan Ibunda Zirdayardanis yang telah melahirkan, membesarkan, mendidik tanpa kenal lelah dan selalu mengalirkan doa untuk penulis.
11. Sahabat-sahabat sholeh yang telah memberi doa untuk penulis secara diam-diam, sehingga Allah ‘Azza Wa Jalla mengabulkan doa tersebut.
12. Teman-teman TIF F 2017 yang tidak bisa penulis sebutkan satu-persatu yang telah berbagi ilmu, memberikan motivasi dan telah membantu dalam masa selama perkuliahan.
13. Semua pihak yang telah membantu dalam proses penulisan tugas akhir ini yang tidak bisa disebutkan satu-persatu.

Semoga laporan tugas akhir ini dapat bermanfaat bagi penulis dan bagi para pembaca. Penulis sadar masih banyak kekurangan dalam penulisan laporan tugas akhir ini. Kritik dan saran dapat dikirimkan melalui alamat email penulis yaitu 11751100101@students.uin-suska.ac.id. semoga Allah

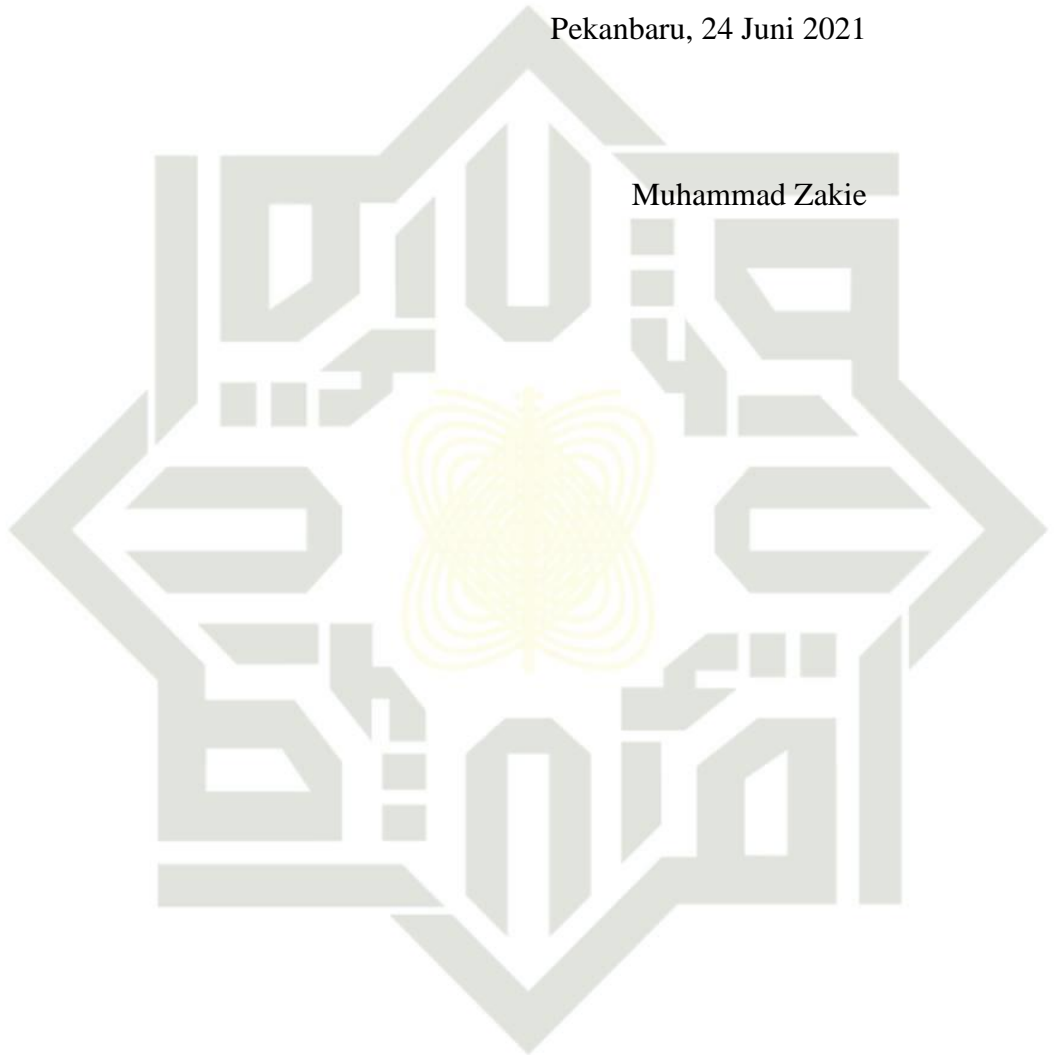


‘Azza Wa Jalla memberikan balasan yang berlimpah kepada semua yang telah membantu penulis. Selamat membaca, semoga bermanfaat.

Wassalamu’alaikum wa rahmatullahi wa barawatuh.

Pekanbaru, 24 Juni 2021

Muhammad Zakie



UIN SUSKA RIAU

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



DAFTAR ISI

LEMBAR PERSETUJUAN	iv
LEMBAR PENGESAHAN	v
LEMBAR HAK KEKAYAAN INTELEKTUAL	ii
LEMBAR PERNYATAN	iii
LEMBAR PERSEMBAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xiv
DAFTAR TABEL	xvi
DAFTAR RUMUS	xvii
DAFTAR SIMBOL	xviii
BAB I PENDAHULUAN.....	I-1
1.1 Latar Belakang	I-1
1.2 Rumusan Masalah	I-3
1.3 Batasan Masalah.....	I-4
1.4 Tujuan Penelitian.....	I-4
1.5 Sistematika Penulisan.....	I-4
BAB II LANDASAN TEORI	II-1
2.1 <i>Blockchain</i>	II-1
2.2 <i>Ethereum</i>	II-4
2.3 <i>Smart Contract</i>	II-5
2.4 <i>Decentralized Application (DApp)</i>	II-6
2.5 <i>E-Voting</i>	II-7
2.6 <i>Kriptografi</i>	II-8

- Hak Cipta Dilindungi Undang-Undang**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

2.6.1	Kriptografi Kunci Simetris.....	II-8
2.6.2	Kriptografi Kunci Asimetris.....	II-9
2.7	Fungsi <i>Hash</i>	II-10
2.7.1	<i>SHA-1</i>	II-11
2.7.2	<i>SHA-2</i>	II-11
2.8	<i>Ganache</i>	II-14
2.9	<i>Truffle Framework</i>	II-15
2.10	<i>Matemask</i>	II-15
2.11	<i>NPM (Node Package Manager)</i>	II-16
2.12	Penelitian Terkait	II-17
BAB III METODOLOGI PENELITIAN		III-1
3.1	Perumusan Masalah.....	III-1
3.2	Studi Pustaka.....	III-2
3.3	Analisa.....	III-2
3.4	Perancangan	III-2
3.5	Implementasi dan Pengujian	III-2
3.5.1	Implementasi	III-2
3.5.2	Pengujian.....	III-2
3.6	Kesimpulan dan Saran.....	III-3
BAB IV ANALISA DAN PERANCANGAN.....		IV-1
4.1	Analisis Proses Bisnis	IV-1
4.2	Desain Arsitektur.....	IV-1
4.2.1	Desain Arsitektur Sistem.....	IV-2
4.2.2	Desain UML <i>Activity Diagram</i>	IV-4
4.2.3	Desain UML <i>Sequence Diagram</i>	IV-8



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

4.3	Mekanisme <i>E-Voting Blockchain</i>	IV-9
4.4	Perancangan Antarmuka	IV-10
4.4.1	Halaman Awal Sistem.....	IV-11
4.4.2	Halaman <i>Login Admin</i>	IV-11
4.4.3	Halaman <i>Dashboard Admin</i>	IV-12
4.4.4	Halaman <i>Data Voters</i>	IV-13
4.4.5	Halaman <i>Admin Hasil Voting</i>	IV-14
4.4.6	Halaman <i>Awal Voter</i>	IV-15
4.4.7	Halaman <i>Hasil Voting</i>	IV-16
BAB V IMPLEMENTASI DAN PENGUJIAN.....		V-1
5.1	Lingkungan Implementasi.....	V-1
5.2	Batasan Implementasi	V-1
5.3	Implementasi Sistem	V-2
5.3.1	Halaman Awal Sistem.....	V-2
5.3.2	Halaman <i>Login Admin</i>	V-2
5.3.3	Halaman <i>Dashboard Admin</i>	V-3
5.3.4	Halaman <i>Data Voters</i>	V-4
5.3.5	Halaman <i>Admin Hasil Voting</i>	V-4
5.3.6	Halaman <i>Awal Voters</i>	V-5
5.3.7	Halaman <i>Hasil Voting</i>	V-6
5.3.8	Pembuatan <i>Smart Contract</i> dengan <i>Blockchain</i> lokal.....	V-6
5.4	Pengujian Sistem	V-11
5.4.1	Pengujian Unit Testing <i>Smart Contract</i>	V-11
5.4.2	Pengujian <i>Fungsionalitas Sistem</i>	V-14
5.4.3	Pengujian <i>Smart Contract Cost</i>	V-22



BAB VI PENUTUP VI-23

6.1 Kesimpulan..... VI-23

6.2 Saran..... VI-23

DAFTAR PUSTAKA xxiv

DAFTAR RIWAYAT HIDUP xxvii



UIN SUSKA RIAU

- Hak Cipta Dilindungi Undang-Undang**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

DAFTAR GAMBAR

Gambar 2. 1	<i>Gambaran nonce pada block untuk membentuk hash</i>	II-2
Gambar 2. 2	Skema Kriptografi Simetris.....	II-9
Gambar 2. 3	Skema Kriptografi Asimetris.....	II-10
Gambar 3. 1	<i>Flowchart</i> Metodologi Penelitian	III-1
Gambar 4. 1	Desain Arsitektur Sistem.....	IV-2
Gambar 4. 2	<i>Smart Contract Development</i> pada <i>Private Testnet</i>	IV-3
Gambar 4. 3	<i>Platform Web</i>	IV-3
Gambar 4. 4	Activity Diagram Proses Login Admin.....	IV-5
Gambar 4. 5	Activity Diagram Input Data Kandidat	IV-6
Gambar 4. 6	Activity Diagram Mulai/Akhiri Voting.....	IV-7
Gambar 4. 7	Activity Diagram Proses Melakukan <i>Voting</i>	IV-8
Gambar 4. 8	<i>Sequence Diagram</i> Sistem.....	IV-9
Gambar 4. 9	Mekanisme <i>E-Voting Blockchain</i>	IV-10
Gambar 4. 10	Halaman Awal Sistem.....	IV-11
Gambar 4. 11	Halaman Login Admin.....	IV-12
Gambar 4. 12	Halaman <i>Dashboard Admin</i>	IV-13
Gambar 4. 13	Halaman Data <i>Voter</i>	IV-14
Gambar 4. 14	Halaman Admin Hasil <i>Voting</i>	IV-15
Gambar 4. 15	Halaman Awal <i>Voter</i>	IV-16
Gambar 4. 16	Halaman Hasil <i>Voting</i>	IV-17
Gambar 5. 1	Halaman Awal Sistem.....	V-2
Gambar 5. 2	Halaman <i>Login Admin</i>	V-3
Gambar 5. 3	Halaman <i>Dashboard Admin</i>	V-3
Gambar 5. 4	Halaman Data <i>Voters</i>	V-4
Gambar 5. 5	Halaman Admin Hasil <i>Voting</i>	V-5
Gambar 5. 6	Halaman Awal <i>Voters</i>	V-5
Gambar 5. 7	Halaman Hasil <i>Voting</i>	V-6
Gambar 5. 8	<i>Blockchain Ethereum Lokal Ganache</i>	V-7
Gambar 5. 9	<i>Compile smart contract</i>	V-10



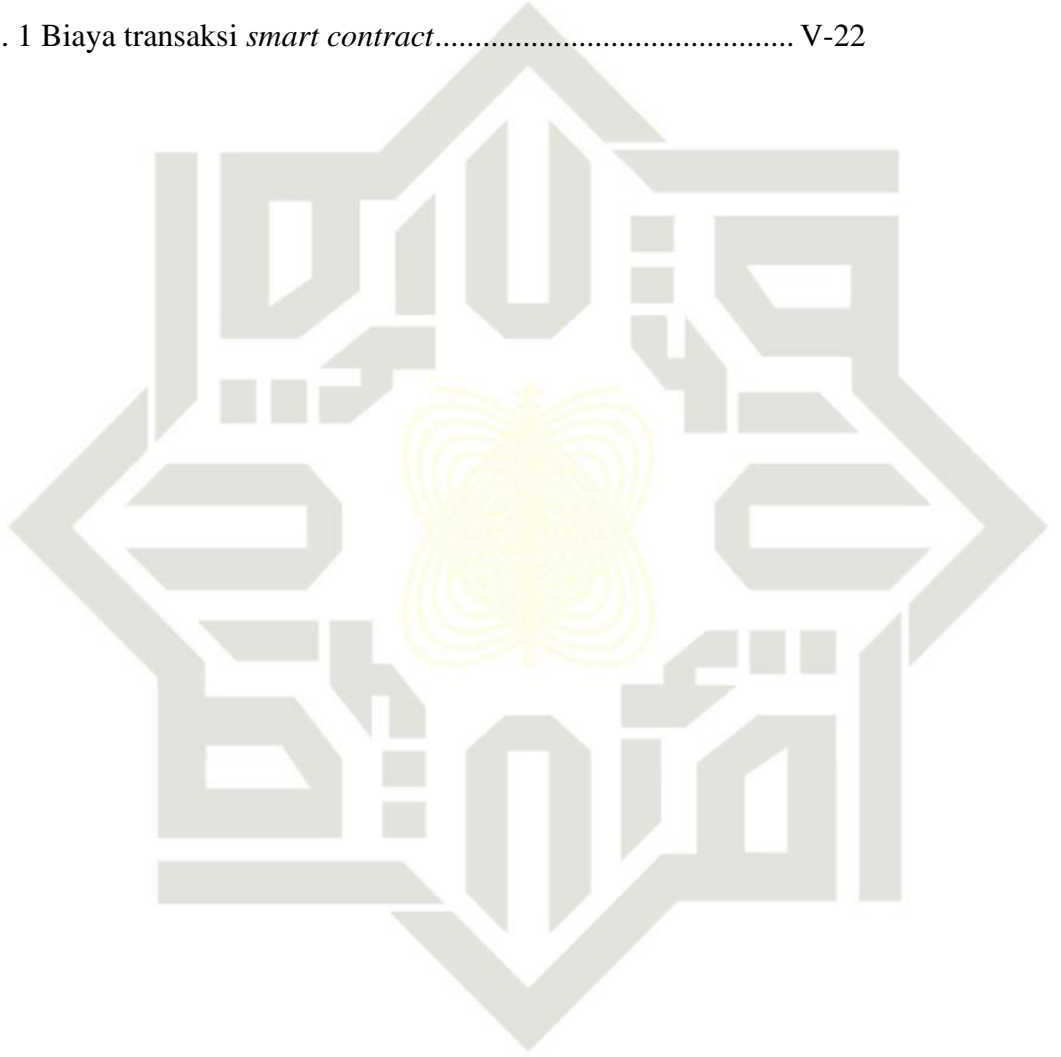
Gambar 5. 10	<i>Migrate smart contract ke blockchain Ethereum lokal..</i>	V-10
Gambar 5. 11	<i>Contracts</i> terdeploy di <i>ganache</i>	V-11
Gambar 5. 12	Unit Testing <i>Smart Contract</i>	V-14
Gambar 5. 13	Konfigurasi <i>account address</i> pada <i>metamask</i>	V-15
Gambar 5. 14	Konfigurasi koneksi <i>account address</i>	V-15
Gambar 5. 15	Konfigurasi <i>metamask</i> untuk koneksi <i>smart contract</i>	V-16
Gambar 5. 16	Peringatan <i>smart contract</i> tidak terdeteksi.....	V-16
Gambar 5. 17	<i>Error</i> transaksi pada <i>metamask</i>	V-17
Gambar 5. 18	Konfirmasi transaksi	V-18
Gambar 5. 19	<i>Blocks</i> transaksi pada <i>ganache</i>	V-19
Gambar 5. 20	Detail <i>block</i> transaksi	V-19
Gambar 5. 21	<i>Events</i> transaksi pada <i>ganache</i>	V-20
Gambar 5. 22	Detail <i>event</i> transaksi pada <i>ganache</i>	V-21
Gambar 5. 23	<i>Transaction</i> pada <i>ganache</i>	V-21

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

DAFTAR TABEL

Table 2. 1 Inisialisasi <i>Hash Value</i>	II-12
Table 2. 2 Konstanta SHA-256	II-14
Table 2. 3 Penelitian Terkait	II-17
Table 5. 1 Biaya transaksi <i>smart contract</i>	V-22



UIN SUSKA RIAU

- Hak Cipta Dilindungi Undang-Undang**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



DAFTAR RUMUS

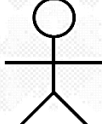


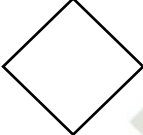

(3. 1) *Smart Contract Cost*..... III-3



UIN SUSKA RIAU

- Hak Cipta Dilindungi Undang-Undang**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

DAFTAR SIMBOL

GAMBAR	NAMA	KETERANGAN
	Aktor	Menspesifikasikan himpunan peran yang pengguna mainkan Ketika berinteraksi.
	Terminator	Symbol terminator (mulai/selesai) merupakan symbol yang menunjukkan permulaan dan akhir dari proses.
	Proses	Symbol yang digunakan untuk melakukan pemrosesan data baik oleh user maupun oleh sistem.
	Verifikasi	Symbol yang digunakan untuk memutuskan apakah valid atau tidak pada suatu kejadian.
	Sistem	Menspesifikasi paket yang menampilkan sistem secara terbatas.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

BAB I PENDAHULUAN

1.1 Latar Belakang

Pemungutan suara atau disebut juga dengan *voting* adalah salah satu tahap untuk melakukan pemilihan umum. Sistem pemungutan suara yang dilakukan di Indonesia masih menggunakan cara manual. (Amelia, Bahri, & Sanjaya, 2018) Bersama dengan berkembang pesatnya ilmu pengetahuan dan teknologi pada saat ini, cenderung mempengaruhi berbagai aktifitas dalam kehidupan manusia. Sangat berguna dan manfaat dengan hadirnya teknologi informasi dan komunikasi yang menjadi solusi dalam bermacam-macam kegiatan yang dilakukan, salah satunya adalah sistem pemilihan. (Palopak, 2018) pemilihan menggunakan teknologi disebut dengan istilah e-voting.

E-Voting adalah proses pemilihan yang memanfaatkan alat elektronik dan dalam proses pemilihannya dilakukan secara *online*. (Ridwan, Arifin, & Yulianto, 2016) Dengan menerapkan sistem *Electronic Voting (E-Voting)*, akan mengatasi masalah pada pemilu konvensional yang menghabiskan banyak biaya untuk penyelenggaraannya yang di mulai dari pendataan pemilih sampai rekapitulasi akhir perhitungan suara. (Ardilla , 2018) Digunakannya *e-voting* adalah agar kecepatan dan akurasi pelaksanaannya meningkat, serta biayanya berkurang. (Prabandari, Bhawiyuga, & Amron, 2019)

Karena kelebihan *e-voting* tersebut dibandingkan dengan pemilihan yang dilakukan dengan cara konvensional menjadi alasan utama mengapa *e-voting* menjadi pilihan utama dalam kegiatan pemilihan. (Prabandari, Bhawiyuga, & Amron, 2019) meskipun begitu, keamanan pada sistem *e-voting* masih sangat diperlukan sistem keamanan yang kuat untuk mengatasi perusakan dan pembobolan data dalam sistem yang dilakukan oleh pihak yang tidak bertanggung jawab. (Ardilla , 2018) beberapa penelitian menyatakan bahwa sistem *e-voting* mempunyai kelemahan dalam penjagaan integritas data saat data tersebut berada dalam *server*. Integritas data dapat dijaga salah satunya dengan

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

menggunakan teknologi *blockchain*, *blockchain* akan menyimpan data secara terdesentralisasi pada jaringan *peer to peer*. (Prabandari, Bhawiyuga, & Amron, 2019)

Blockchain atau disebut dengan teknologi pembukuan yang terdistribusi (*Distributed Ledger Technology/DLT*) adalah suatu rancangan tergabungnya setiap orang ke dalam jaringan dan memiliki hak untuk akses terhadap pembukuan terdistribusi. Rancangan database terdistribusi merupakan contoh dari rancangan bawaan dari *blockchain* yang telah ada sebelumnya dan muncul bersamaan dengan munculnya *bitcoin* yang merupakan jawaban dari masalah keyakinan diantara pihak ketiga (institusi finansial/pemerintah) dengan pihak-pihak yang terlibat dalam transaksi di kawasan yang tidak aman. (Noorsanti, Yulianton, & Hadiono, 2018)

Blockchain merupakan solusi berbentuk *database* yang terdesentralisasi dan terdistribusi yang melindungi data yang tidak berhenti bertambah setelah setiap *node* berperan dalam konfirmasi data. *peer* akan melacak dan menahan data tersebut diproses lebih lanjut bila menemukan perbedaan antara salinan data di salah satu *peer*. Transaksi disimpan pada *chain* berbentuk *block* yang disimpan bersifat permanen, transparan, dan dapat ditelusuri, supaya setiap *peer* memungkinkan untuk melacak seluruh riwayat transaksi. (Prabandari, Bhawiyuga, & Amron, 2019)

Setelah *block* data telah terbentuk dan *block* data sudah tergabung dalam jaringan untuk divalidasi, maka *block* baru bertambah setelah *node* tersebut tersimpan ke dalam rantai *block* yang sudah ada. (Aprialim, Adnan, & Paundu, 2017) *Blockchain* pada sistem *ethereum* sangat cocok untuk diterapkan, karena konsistensi penggunaannya yang luas dan menyediakan logika *smart contract*. (Setia & Susanto, 2019)

Smart Contract adalah sebuah program komputer kecil yang tersimpan ke dalam jaringan *blockchain* secara efektif. Transaksi yang dibuat oleh program kecil tersebut akan melakukan hal yang sudah ditentukan sejak awal dan tidak bisa diubah lagi. Tidak sama dengan kontrak biasa harus mengeksekusi isi kontrak setelah mencapai kesepakatan. Oleh karena itu kontrak yang cerdas adalah *self*

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

executing yaitu, transaksi akan berlangsung secara otomatis setelah diperintah ke *blockchain* saat kondisi yang sesuai terdeteksi, tanpa adanya campur tangan dari para pihak yang bertransaksi atau pihak ketiga lainnya. (Nugraha, 2020) Untuk melakukan transaksi ke jaringan *blockchain ethereum*, maka diperlukan biaya agar data bisa di simpan ke dalam jaringan *blockchain ethereum*.

Ethereum blockchain menggunakan bahasa pemrograman *solidity* untuk menerapkan *smart contract* yang diketik dan disimpan dalam *file* berekstensi *.sol*, dan mempunyai kemiripan syntax dengan *javascript*. *Smart contract* berbentuk sama seperti kelas pada bahasa pemrograman *object oriented*. Semua pekerjaan dijalankan secara *real time*, dan dengan biaya beberapa Ether (mata uang dari jaringan *Ethereum*) ditulis semua blok pada rantai pamungkas sebagai hadiah kepada para penambang, yang telah melakukan pekerjaan penulisan dan validasi dalam hal waktu dan kekuasaan perhitungan yang mahal. (Setia & Susanto, 2019)

Solusi yang dapat dilakukan untuk dapat mengatasi masalah keamanan dan integritas data pada sistem *e-voting* adalah menerapkan teknologi *blockchain*. Dengan menerapkan teknologi *blockchain* maka data akan aman karena setiap transaksi yang dilakukan akan di enkripsi menggunakan *Secure Hash Algorithm 256 (SHA-256)*, dan akan terbentuk blok yang bersambung dan dikirimkan ke seluruh jaringan yang terkoneksi ke jaringan *blockchain* secara *peer to peer* sehingga semua memvalidasi transaksi tersebut dan tidak membutuhkan server tunggal untuk menyimpan datanya. (Ardilla , 2018) Pada penelitian ini, penulis akan mengimplementasikan teknologi *blockchain* menggunakan bahasa *solidity* untuk membuat *smart contract* yang dilakukan menggunakan jaringan *blockchain ethereum* lokal yaitu *ganache* dimana untuk bisa bertransaksi dengan *ganache* membutuhkan biaya berupa gas yang dilakukan pada studi kasus *e-voting*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka penulis mengambil rumusan masalah “bagaimana mengimplementasikan teknologi *blockchain* menggunakan *smart contract* pada *e-voting*”.



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

1.3 Batasan Masalah

Batasan masalah bertujuan untuk menghindari pembahasan yang melebar dari pokok permasalahan. Berdasarkan rumusan masalah di atas maka dibatasi masalah yaitu:

1. Ruang lingkup dari penggunaan sistem ini hanya untuk mengimplementasikan teknologi *blockchain* pada studi kasus *e-voting*.
2. Sistem yang akan dibangun hanya untuk mengimplementasi integritas data pada *blockchain ethereum*.
3. Sistem yang akan dibangun berbasis web menggunakan bahasa *solidity* untuk membuat *smart contract*.
4. Menggunakan *blockchain ethereum* lokal yaitu *ganache*.
5. Pehitungan biaya *smart contract* hanya pada transaksi yang dilakukan di *blockchain ethereum* lokal *ganache*.
6. *Browser* yang digunakan harus sudah mendukung *extension metamask*.

1.4 Tujuan Penelitian

Tujuan dari penelitian tugas akhir ini adalah mengimplementasikan teknologi *blockchain* menggunakan *smart contract* pada *e-voting*.

1.5 Sistematika Penulisan

Dalam penyusunan laporan ini, penulis menggunakan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi deskripsi umum dari tugas akhir yang meliputi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan laporan Tugas Akhir.

BAB II LANDASAN TEORI

Bab ini menjelaskan tentang teori-teori yang berasal dari jurnal dan buku yang berkaitan dengan studi kasus pada penelitian Tugas Akhir ini.

BAB III METODOLOGI PENELITIAN

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Bab ini berisi tentang metodologi penelitian tugas akhir yaitu tahapan tahapan dalam membuat sistem penelitian Tugas Akhir mulai dari tahapan perumusan masalah, pengumpulan data, analisa dan perancangan, implementasi dan pengujian, hingga kesimpulan dan saran dari hasil penelitian tugas akhir.

BAB IV ANALISA DAN PERANCANGAN

Pada bab ini berisi tentang analisa dari aplikasi yang akan dibangun dan yang digunakan dalam Tugas Akhir ini.

BAB V IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi dan perancangan yang telah dibuat sebelumnya, yaitu meliputi implementasi basis data, implementasi metode yang akan digunakan dan hasil pengujian terhadap sistem.

BAB VI PENUTUP

Bab ini berisi tentang kesimpulan dan saran hasil penelitian Tugas Akhir yang telah dilakukan.

BAB II

LANDASAN TEORI

2.1 *Blockchain*

Blockchain merupakan rantai yang terbentuk dari sekumpulan *block* dimana setiap *block* memiliki 3 bagian berupa data, nilai *hash* dari *blok*, dan nilai *hash* dari *block* sebelumnya. Setiap data yang tersimpan dalam *block* bergantung pada tipe *block*, contohnya *blockchain* pada *bitcoin* yang datanya berisi detail transaksi seperti penerima, pengirim, dan nilai koin. (Noorsanti, Yulianton, & Hadiono, 2018)

Blockchain merupakan buku besar terdistribusi yang menyediakan cara supaya informasi bisa tersimpan dan dibagikan oleh suatu komunitas. Setiap anggota pada komunitas ini dapat saling menyimpan informasi mereka, dan terjadi validasi pembaruan oleh semua anggota. Informasi pada *blockchain* berupa transaksi, kontrak asset, identitas, atau semua yang bisa diterangkan berupa bentuk digital. Datanya bersifat permanen, transparan dan dapat dicari, yang dapat melihat riwayat transaksi secara keseluruhan oleh semua anggota komunitas. Setiap pembaruan adalah *block* baru yang ditambahkan ke akhir rantai/*chain*. (Nugraha, 2020)

Teknologi *blockchain* mempunyai karakteristik yang bisa dirangkai dari penelitian sebelumnya adalah sebagai berikut (Noorsanti, Yulianton, & Hadiono, 2018):

1. Terdistribusinya pembukuan pada jaringan *peer-to-peer* yang mana proses pembukuan tersebut merupakan sebuah proses yang selalu melakukan verifikasi. Pembukuan tersebut juga bisa diakses oleh semua anggota yang tergabung didalam jaringan tersebut.
2. Informasinya yang permanen, tidak bisa berubah dan aman dari perubahan karena mempunyai langkah verifikasi serta informasi yang sama pada semua simpul.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang

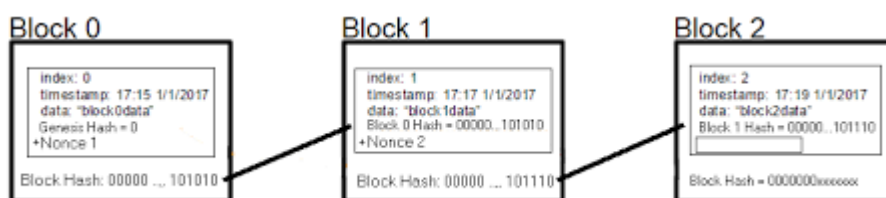
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

3. Transparansinya informasi yang tersimpan didalam jaringan *blockchain* untuk semua anggota yang tergabung tetapi tidak bisa informasi tersebut diubah.
4. Mempunyai *smart contracts* yang secara otomatis melakukan eksekusi dan verifikasi agar tersimpannya semua kebijakan dan aturan yang akan dipakai saat negosiasi ketentuan kontrak.

Blockchain memiliki sifat yang *append-only*, *nd-only*, adalah *blockchain* hanya bisa menambahkan data terbaru, adapun data-data yang sudah ditambahkan tidak bisa lagi diubah maupun dihapus. *Blockchain* merupakan kumpulan data yang terdistribusi dan terdesentralisasi yang menjamin keamanan data-nya. Selanjutnya penjelasan tentang bagaimana *blockchain* mampu memelihara data *append-only* ini, khususnya dengan cara memakai *proof-of-work* dan *longest-chain consensus*. (Alvaro , 2018)

Mula-mula akan diterangkan bagaimana cara pertambahan suatu *block* ke *blockchain*. Saat pertambahan *block* ke *blockchain*, *hash* dari *block* tertentu wajib mencukupi suatu syarat, yakni *n* karakter awal dari *hash*-nya wajib merupakan karakter tertentu. Contohnya *hash* “0000727ea4009f7c463475a9a1eb87ef”, yang mana mempunyai 4 karakter *hash* pertamanya adalah angka 0. Nilai *n* adalah penentu tingkat kesulitan dari *blockchain*, apabila nilai *n* semakin tinggi, maka akan semakin sulit pula *hash* ditemukan. (Alvaro , 2018)

Tidak ada kepastian bahwa *hash* dari *block* bisa terpenuhi syarat tersebut karena suatu *block* mengandung data khusus, maka dengan itu *nonce* tersebut bertambah, merupakan suatu angka yang bisa menciptakan *hash* dari *block* dan terpenuhinya syarat tersebut. (Alvaro , 2018)



Gambar 2. 1 Gambaran nonce pada block untuk membentuk hash

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

- a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
- b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Seperti itulah Syarat *hash* yang dinamakan dengan *proof-of-work*. Karena *hashing* adalah fungsi satu arah, satu-satunya cara untuk mendapatkan *hash* yang memenuhi *proof-of-work* adalah dengan memaksanya menemukan nomor acak yang membuat *hash* blok memenuhi *proof-of-work*. Operasi ini secara komputasi mahal, terutama di bawah kesulitan tinggi. Oleh karena itu, bukti kerja adalah cara bagi *blockchain* untuk mempersulit *blockchain* untuk menambah dan mengonversi blok. (Alvaro , 2018)

Selanjutnya, penjelasan bagaimana setiap *node* di jaringan *blockchain* beradaptasi dengan *blockchain*-nya. Intinya, *blockchain* di jaringan terpanjang dianggap paling otoritatif. Tentu saja, periksa dulu validitas setiap *blockchain* dengan memeriksa *hash*-nya seperti yang dijelaskan di atas. Ketika sebuah *node* ingin menambahkan blok, pertama-tama ia akan menemukan *blockchain* terpanjang di jaringan untuk memperbarui *blockchain*-nya. Setelah itu, blok ditambahkan ke *blockchain*. *Node* harus melakukan ini karena *blockchain* terpanjang adalah yang paling otoritatif, sehingga perlu membuat *blockchain* terpanjang untuk diterima oleh *node* lain di jaringan. (Alvaro , 2018)

Jika seseorang mengubah blok B₁ dengan serangan, nilai *hash* dari blok itu juga akan berubah, jadi dia harus mengubah isi dari nilai *hash* blok B₂ sebelumnya. Oleh karena itu, nilai *hash* blok B₂ juga akan berubah, sehingga nilai *hash* sebelumnya dari blok B₃ juga harus diubah, begitu seterusnya hingga blok terakhir. Harus ditekankan bahwa mengubah isi blok akan mengubah *hash*, sehingga penyerang harus menemukan nomor acak baru untuk memenuhi bukti kerja untuk seluruh blok yang dimodifikasi, yang secara komputasi sangat sulit. Selain itu, *blockchain* yang dianggap valid harus diterima oleh mayoritas *node*. Oleh karena itu, penyerang harus secara bersamaan menyerang sebagian besar *node* di jaringan *blockchain* dan pencarian bukti kerjanya. Karena ini sulit dilakukan, inilah mengapa *blockchain* sangat aman sebagai buku besar terdistribusi tambahan, yaitu begitu data masuk ke jaringan *blockchain*, sulit untuk diubah atau dihapus. (Alvaro , 2018)

Keamanan data adalah salah satu perhatian utama teknologi *blockchain*. Data pada *blockchain* dilindungi oleh *multi-layer* dan teknologi sekunder seperti *hash*,

rantai *hash*, kunci publik dan pribadi, dan distribusi data P2P. Hal ini membuat teknologi *blockchain* sangat cocok dan sangat cocok untuk menyimpan data publik yang rentan terhadap manipulasi. Salah satu contohnya adalah data identitas demografi, yaitu data yang rentan terhadap manipulasi dan serangan *hacker* oleh pihak-pihak yang tidak bertanggung jawab sehingga harus disimpan dengan cara yang sangat aman, namun pada saat yang sama harus mudah diakses oleh publik untuk berbagai akses. Tujuannya, seperti verifikasi data. Jadi ini membuat teknologi *blockchain* cocok untuk menyimpan data semacam ini. (Yeni & Kumala)

2.2 Ethereum

Awal mula munculnya *Ethereum* yaitu pada tahun 2013 yang dikembangkan oleh Vitalik Buterin. *Ethereum* didefinisikan sebagai salah satu penerapan dari *blockchain* yang memiliki kesanggupan untuk melakukan komputasi dalam pemanfaatan *blockchain* yang mana sebelumnya hanya bisa melaksanakan tukar-menukar mata uang digital dan sebagai asset digital antar pengguna. (Badawi)

Ethereum merupakan *cryptocurrency* kedua yang terbesar dari semua kapitalisasi pasar yang memiliki dokumentasi ekstensif dan komunitas pengembang aktif. *Ethereum blockchain* adalah program komputasi terdistribusi sumber terbuka yang mengamati kegunaan *smart contract*. (Dzulfikar & Susanto, 2020)

Ethereum pada *bitcoin* adalah *hyper ledger* dari *cryptocurrency blockchain* publik. Hal terpenting adalah *blockchain bitcoin* hanya menyimpan transaksi yang diperdagangkan *bitcoin* antar alamat, meskipun *Ethereum Blockchain* menyimpan alamat dengan kode EVM. Transaksi yang dicatat di *blockchain* adalah panggilan kode yang direferensikan diatas, dan berisi data tentang informasi yang masuk ke program sebagai input. Proyek-proyek ini diinterpretasikan oleh mesin virtual terbatas yang disebut *Ethereum Virtual Machine (EVM)* yang di ekspresikan dalam Bahasa yang sesuai. (Dzulfikar & Susanto, 2020)

Di bagian ini, beberapa konsep *ethereum* dasar dijelaskan: akun, transaksi, dan klien. Unit dasar *ethereum* adalah akun. Akun diperlukan untuk semua orang

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

yang ingin mengirim transaksi apa pun ke *blockchain*. *Ethereum* sendiri mencakup dua jenis akun yaitu: Akun Milik Eksternal (EOA), pengguna langsung mengirim transaksi melalui mereka, dan Akun Kontrak, yang didasarkan pada kode kontrak jika perlu memanggil kontrak lain kemudian mengirim transaksi internal. Akun pada *Ethereum* terbagi menjadi dua kunci, yaitu kunci pribadi dan kunci publik. Setiap alamat akun berasal dari 20 *byte*. (Dzulfikar & Susanto, 2020)

Untuk melakukan transaksi ke *ethereum* maka dibutuhkan biaya yang disebut dengan gas. Gas adalah Sebagian yang terdapat pada ether dan digunakan untuk melakukan proses mining yang dilakukan oleh *miners*. Proses mining adalah proses yang dilakukan guna untuk menyimpan suatu transaksi dalam suatu blok dan menambahkan blok ke *blockchain*. (Sabrina, Budiyo, & Widjarto, 2019)

Semakin kompleks sebuah transaksi, maka biaya transaksinya akan semakin mahal. Total biaya transaksi bergantung pada hasil kali antara ukuran *gas* yang dipakai, nilai *gas limit per byte*, dan *gas price*. Nilai dari *gas limit per byte* bersifat tetap dan ditentukan oleh kode program *blockchain*. Sedangkan nilai pada *gas price* ditentukan oleh pengirim dengan nilai minimal 1 Gwei (*giga wei*, 1 *wei* = satu per-milyar Ether). Nilai *gas price* juga menentukan kecepatan transaksi yang akan tercatat ke dalam jaringan *blockchain*. Biaya transaksi ditentukan oleh seberapa besar ukuran dari transaksi yang dikirim dengan cara menyesuaikan nilai dari *gas limit* pada transaksi. (Sidiq, Basuki, Firdaus, & Baihaqi, 2020)

2.3 Smart Contract

Smart Contract adalah program komputer yang dijalankan melalui transaksi *blockchain* yang dapat mempertahankan status, berinteraksi dengan *cryptocurrency* dengan cara yang terdesentralisasi, dan mengambil masukan pengguna. *Smart Contract* ditulis dalam bahasa pemrograman *Solidity*, yang merupakan campuran *C++* dan *JavaScript*. *Smart Contract* dikendalikan oleh rekan-rekan dari organisasi *Ethereum* secara berkala, dan mereka harus disetujui oleh dua klien berbeda untuk dimulai. Sejak saat itu, fungsi kontrak dapat

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

dijalankan, dan kontrak dapat diberikan kepada pelamar yang berbeda. (Dzulfikar & Susanto, 2020)

Solidity adalah bahasa pemrograman berorientasi obyek yang mempunyai fungsi untuk menciptakan *smart contract* agar dapat dijalankan pada *Ethereum Virtual Machine* (EVM), dan disimpan dalam ekstensi (.sol). Seluruh kode bahasa pemrograman *Solidity* akan dikompilasi menggunakan *Solidity compiler* atau disebut juga dengan “solc” yang menghasilkan *bytecode* (sekumpulan fungsi yang telah diencode). (Badawi)

Smart Contract merupakan sebuah langkah untuk menyimpan seluruh kebijakan dan ketentuan yang akan dipakai saat negosiasi penentuan kontrak. Hal tersebut merupakan langkah yang secara otomatis melaksanakan verifikasi dan eksekusi agar setiap anggota tercapai pada saat konsensus. (Noorsanti, Yulianton, & Hadiono, 2018) *Smart contract* bertujuan agar terkelola siklus lengkap pada *smart contract* yang legal. (Ariefa & Sundarab, 2017)

2.4 *Decentralized Application (DApp)*

DApp yang diterapkan tidak memerlukan pemeliharaan dan tata kelola dari pengembang aslinya. Dengan kata lain, aplikasi atau layanan *blockchain* yang ideal harus dapat dioperasikan tanpa campur tangan manusia, yang membentuk Organisasi Otonomi Terdesentralisasi (DAO). DAO adalah organisasi yang dijalankan melalui aturan yang dikodekan sebagai *smart contract* yang berjalan di *blockchain*. Karena sifatnya yang otonom dan otomatis, biaya dan keuntungan DAO dibagi oleh semua peserta hanya dengan mencatat semua aktivitas ke dalam blok. Menurut definisi *DApp* ditandai oleh empat properti sebagai berikut:

- 1) Sumber Terbuka: Karena sifat *blockchain* yang tepercaya, *DApp* perlu membuat kodenya menjadi sumber terbuka, sehingga audit dari pihak ketiga menjadi mungkin.
- 2) Dukungan *cryptocurrency* internal: Mata uang internal adalah kendaraan yang menjalankan ekosistem untuk *DApp* tertentu. Dengan token, *DApp* dapat mengukur semua kredit dan transaksi di antara peserta sistem, termasuk penyedia konten dan konsumen.
- 3) Desentralisasi adalah dasar dari transparansi.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

- 4) Tidak ada titik kegagalan: Sistem yang sepenuhnya terdesentralisasi seharusnya tidak memiliki titik pusat kegagalan karena semua komponen aplikasi akan dihosting dan dijalankan di *blockchain*. (Cai, et al., 2018)

2.5 E-Voting

Semakin pesatnya perkembangan teknologi menyebabkan banyak sekali sistem yang berkembang salahsatu contohnya adalah voting. Dimana sebelumnya orang melakukan voting dengan cara menggunakan kertas dan dihitung secara manual, sedangkan saat ini orang melakukan voting dapat menggunakan media elektronik yang disebut sebagai *e-voting*. (Prasetyo & Munir)

Voting merupakan sebuah metode untuk menyatukan aspirasi dengan cara pengambilan keputusan dalam mendapatkan jalan keluar terbaik agar suatu permasalahan dapat terselesaikan. Salah satu contoh dari menerapkan teknologi informasi yang terus berkembang sangat pesat adalah *e-voting* yang dapat mengatasi suatu masalah yang muncul dari pelaksanaan pemilihan umum yang diselenggarakan secara manual. (Tjandra & Setiyawati, 2019)

E-Voting (Electronic Voting) pertama kali diperkenalkan oleh David Shaumm pada awal tahun 1980. Sistem yang digunakan adalah dengan menggunakan *cryptography-key* yang membantu agar tidak terdeteksinya para *voter*. Estonia adalah negara yang pertama kali menggunakan electronic voting hanya menggunakan internet dan kartu tanda penduduk elektronik (e-KTP). Norwegia adalah negara selanjutnya yang mengimplementasikan electronic voting. Sistem yang dibuat mirip seperti yang dimiliki Estonia, tetapi terpaksa tidak diteruskan karena banyak pihak yang takut akan keamanan dari sistem itu. Washington D.C juga mengembangkan *electronic voting* pada tahun 2010. Tetapi banyak sekali masalah keamanan pada saat melakukan pengujian pada sistemnya. Sehingga proyek tersebut tidak pernah diimplementasikan. (Hu, Palit, & Handojo)

Pengertian secara umum *e-voting* adalah suatu metode menggunakan teknologi berupa perangkat elektronik untuk melakukan pemungutan suara yang mana penerapan-nya sangat berbeda, contohnya penggunaan aplikasi berbasis website sebagai otentikasi pemilih, aplikasi berbasis *android* sebagai sistem pemungutan suara, untuk mengganti kertas suara maka digunakan penggunaan

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

touch screen, dan sangat banyak lagi teknologi yang dapat diterapkan. (Muid, Sholihin, & Wardhani, 2017)

2.6 Kriptografi

Kata *kriptografi* berasal dari bahasa Yunani yaitu, *crypto* dan *graphia* yang mempunyai arti *writing* (tulisan). Berdasarkan istilahnya, *kriptografi* merupakan ilmu dan seni untuk terjaganya keamanan pada pesan saat pesan dikirim dari sebuah tempat ke tempat yang lain. (Sugiyatno & Atika, 2018)

Awal mulanya *kriptografi* muncul dari orang-orang mesir melalui *hieroglyph* 4000 tahun yang lalu. Dikisahkan pada saat pengiriman pesan rahasia dari Jalius Caesar yang tidak menginginkan pesan tersebut terbuka di jalan melalui perantara seorang kurir kepada seorang jendral di medan perang. Cara untuk bisa mengatasi hal tersebut adalah mengacak pesan hingga menjadi pesan yang hanya bisa dipahami oleh jendralnya saja karena sudah diberitahu sebelumnya. Caranya mengetahui arti pesan acak tersebut adalah mengubah susunan *alfabet* dari a, b, c yaitu a menjadi d, b menjadi e, dan c menjadi f dan seterusnya. Dari penjelasan tersebut, *enkripsi* adalah yang dilakukan Julius Caesar dengan mengacak pesan. *dekripsi* adalah saat sang jendral merapikan pesan yang teracak. *plaintext* adalah pesan awal yang belum diacak dan pesan yang telah dirapikan, sedangkan *chipertext* adalah pesan yang sudah teracak. (Sugiyatno & Atika, 2018)

2.6.1 Kriptografi Kunci Simetris

Algoritma ini bisa mengirim dan menerima pesan yang kuncinya sudah diketahui sebelum dikirim. Algoritma simetris adalah algoritma yang menggunakan kunci enkripsi dan kunci dekripsi yang sama, sehingga algoritma ini disebut algoritma kunci tunggal. Keamanan pesan menggunakan algoritma ini tergantung pada kuncinya, karena jika orang lain mengetahui kuncinya, orang tersebut dapat mengenkripsi dan mendekripsi pesan tersebut. (Sugiyatno & Atika, 2018)

Algoritma menggunakan kunci simetris meliputi (Sugiyatno & Atika, 2018) :

Hak Cipta Dilindungi Undang-Undang

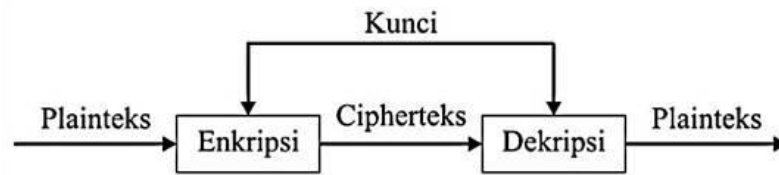
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

1. *Data Encryption Standard* (DES)
2. *RC2, RC4, RC5, RC6*
3. *International Data Encryption Algorithm* (IDEA)
4. *Advanced Encryption Standard* (AES)
5. *One Time Pad* (OTP)

Berikut Ilustrasi penggunaan algoritma kriptografi simetris:



Gambar 2. 2 Skema Kriptografi Simetris

: Sebelum mengirim pesan, pengirim dan penerima memilih kunci yang sama untuk digunakan bersama, dan kuncinya adalah rahasia.

2.6.2 Kriptografi Kunci Asimetris

Kriptografi kunci asimetris juga disebut kriptografi kunci publik. Enkripsi dan dekripsi menggunakan kunci yang berbeda, setiap orang yang berkomunikasi memiliki pasangan kunci, yaitu (Sugiyatno & Atika, 2018) :

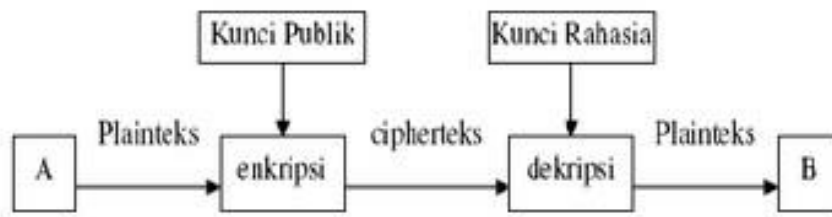
1. Kunci umum (*public key*) adalah kunci yang dapat diketahui semua orang.
2. Kunci rahasia (*private key*) adalah kunci rahasia atau kunci yang hanya diketahui oleh satu orang.

Kunci-kunci ini saling terkait. Bahkan jika Anda mengetahui kunci publik, sulit untuk mengetahui kunci privat mana yang digunakan. Contoh algoritma kriptografi kunci publik termasuk RSA, Elgamal, DSA, dll.. (Sugiyatno & Atika, 2018)

Berikut ini adalah ilustrasi penggunaan algoritma enkripsi asimetris :

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Gambar 2. 3 Skema Kriptografi Asimetris

2.7 Fungsi Hash

Fungsi *hash* adalah metode atau cara untuk menghasilkan "sidik jari" digital kecil dari data apa pun [1,2,3]. Fungsi ini memecahkan dan mencampur data untuk menghasilkan sidik jari, yang biasanya disebut nilai *hash* dan biasanya diwakili oleh string pendek huruf dan angka acak (heksadesimal). Fungsi *hash* yang baik adalah fungsi (jarang) yang tidak memiliki output nilai *hash* yang sama untuk input yang berbeda. (Sugiyatno & Atika, 2018)

Fungsi *hash* biasanya disebut sebagai fungsi satu arah, intisari pesan, sidik jari, kompresi, dan kode verifikasi pesan. Fungsi ini biasanya digunakan untuk mendapatkan sidik jari dari sebuah pesan. Fungsi *hash* adalah fungsi yang menerima *string* input dengan panjang berapa pun dan mengubahnya menjadi *string* output dengan panjang tetap. (Sugiyatno & Atika, 2018)

Fungsi *hash* h memiliki sifat-sifat sebagai berikut (Sugiyatno & Atika, 2018):

1. *Preimage resistant*

Apabila diberikan suatu nilai hash y , maka akan sulit mencari M sedemikian sehingga $h(M) = y$

2. *Second preimage resistant*

Apabila diberikan sebuah masukan M , maka akan sulit mencari M' sedemikian sehingga $h(M) = h(M')$

3. *Collision resistant*

Akan sulit untuk mencari M dan M' sedemikian sehingga $h(M) = h(M')$

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

2.7.1 SHA-1

SHA adalah bagian dari fungsi hash satu arah. SHA-0 adalah bagian paling awal dari SHA, hanya disingkat SHA, dirilis pada tahun 1993. Diikuti oleh SHA-1 yang dirilis pada tahun 1995. SHA-224, SHA-256, SHA-384, SHA-512 adalah empat varian lain yang dirilis dan keempat varian tersebut disebut SHA-2. (Wandani & Sinurat, 2018)

Pada tahun 1993, SHA dikembangkan oleh *National Institute of Standards and Technology* (NIST) dan diterbitkan sebagai *Federal Information Processing Standard* (FIPF 180). *Secure Hash Standard* (SHS) menetapkan bahwa SHA-1 digunakan untuk menghitung nilai hash dari pesan atau file. Panjang pesan maksimum SHA-1 adalah 264 bit, dan outputnya adalah 160 bit, yang disebut intisari pesan atau kode *hash*. (Kurniawan, Kusyanti, & Nurwarsito, 2017)

2.7.2 SHA-2

SHA-2 banyak variannya dan yang paling populer adalah SHA-256, yang mana bitcoin menggunakan SHA-256.

Secure Hash Algorithm (SHA) 256 adalah fungsi *hash* yang umum digunakan, dan belum ada yang dapat memecahkan algoritma fungsi *hash* SHA-256. (Saputra & Nasution, 2019) Algoritma SHA-256 memiliki 8 tahap tahapan kerja sebagai berikut:

- a. Tambahkan bit *Padding*
Isi pesan sehingga panjangnya konsisten dengan 448 modulo 512. Tambahkan 1 bit *padding* di akhir pesan, diikuti dengan jumlah nol yang diperlukan, sehingga panjang bit sama dengan 448 modulo 512.
- b. Panjang *Append*
Panjang pesan 64-bit ditambahkan, langkah ini membuat panjang pesan menjadi kelipatan 512 bit.
- c. *Parsing* pesan
Mengurai pesan pesan isian diurai menjadi N blok pesan 512-bit, blok $M(1), M(2), \dots, M(N)$, dan 64-bit ditambahkan.
- d. Inisialisasi Nilai *Hash*

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Inisialisasi nilai *hash* awal $H(0)$ diatur dan terdiri dari 8 kata 32-bit dalam format heksadesimal.

Table 2. 1 Inisialisasi Hash Value

Variabel	Hash value
$H_0^{(0)}$	= 6A09E667
$H_1^{(0)}$	= BB67EA85
$H_2^{(0)}$	= 3C6EF372
$H_3^{(0)}$	= A54FF53A
$H_4^{(0)}$	= 510E527F
$H_5^{(0)}$	= 9B05688C
$H_6^{(0)}$	= 1F83D9AB
$H_7^{(0)}$	= 5BE0CD19

e. Mempersiapkan jadwal pesan

SHA-256 menggunakan penjadwalan pesan 32-bit 64-kata, dan kata-kata penjadwalan pesan ditandai sebagai W_0, W_1, \dots, W_{63} .

$W_t =$

$$\begin{cases} M_t^{(t)} & 0 \leq t \leq 15 \\ \sigma_1^{(256)}(W_{i-2}) + W_{i-7} + \sigma_0^{(256)}(W_{i-15}) + W_{i-16} & 16 \leq t \leq 63 \end{cases} \quad (1)$$

Di mana :

$$\begin{aligned} \sigma_1^{(256)}(W_{i-2}) &= ((W_{i-2})ROTR 17) \oplus ((W_{i-2})ROTR 19) \\ &\oplus ((W_{i-2})SHR 10) \end{aligned} \quad (2)$$

$$\begin{aligned} \sigma_0^{(256)}(W_{i-15}) &= ((W_{i-15})ROTR 7) \oplus ((W_{i-15})ROTR 18) \\ &\oplus ((W_{i-15})SHR 3) \end{aligned} \quad (3)$$

Keterangan:

- W_t = Blok pesan yang baru
- M_t = Blok pesan yang lama
- W_{i-2} = Blok pesan dari W ke $i-2$
- W_{i-15} = Blok pesan dari W ke $i-15$

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

ROTR = Rotate Right

SHR = Shift Right

\oplus = Operator XOR

f. Inisialisasi delapan variabel kerja a, b, c, d, e, f, g, dan h dengan nilai *hash* (i-1)

For t=0 to 63

{

$$T_1 = h + \sum_1^{(256)}(e) + Ch(e, f, g) + K_1^{(256)} + W_t \quad (4)$$

$$T_2 = \sum_0^{(256)}(a) + Maj(a, b, c) \quad (5)$$

$$h = g \quad (6)$$

$$g = f \quad (7)$$

$$f = e \quad (8)$$

$$e = d + T_1 \quad (9)$$

$$d = c \quad (10)$$

$$c = b \quad (11)$$

$$b = a \quad (12)$$

$$a = T_1 + T_2 \quad (13)$$

Di mana:

$$\sum_1^{(256)}(e) = (e \text{ ROTR } 6) \oplus (e \text{ ROTR } 11) \oplus (e \text{ ROTR } 25)$$

$$\sum_0^{(256)}(e) = (e \text{ ROTR } 2) \oplus (e \text{ ROTR } 13) \oplus (e \text{ ROTR } 22)$$

$$Ch(e, f, g) = (e \wedge f) \oplus (\sim e \wedge g)$$

$$Maj(a, b, c) = (a \wedge b) \oplus (a \wedge c) \oplus (b \wedge c)$$

a, b, c, d, e, f, g, h = variabel yang berisi pesan heksadesimal

$K_1^{(256)}$ = Konstanta SHA-256

ROTR = Rotate Right

\oplus = Operator XOR

\wedge = Operator AND

Table 2. 2 Konstanta SHA-256

478A2F98	71374491	B5C0FBCF	E9B5DBA5	3956C25B	59F111F1	923F82A4	AB1C5ED5
D807AA98	12835B01	243185BE	550C7DC3	72BE5D74	80DEB1FE	9BDC06A7	C19BF174
E49B69C1	EFBE4786	0FC19DC6	240CA1CC	2DE92C6F	4A7484AA	5CB0A9DC	76F988DA
983E5152	A831C66D	B00327C8	BF597FC7	C6E00BF3	D5A79147	06CA6351	14292967
27B70A85	2E1B2138	4D2C6DFC	53380D13	650A7354	766A0ABB	81C2C92E	92722C85
A2BFE8A1	A81A664B	C24B8B70	C76C51A3	D192E819	D6990624	F40E3585	106AA070
19A4C116	1E376C08	2748774C	34B0BCB5	391C0CB3	4ED8AA4A	5B9CCA4F	682E6FF3
748F82EE	78A5636F	84C87814	8CC70208	90BEFFFA	A4506CEB	BEF9A3F7	C67178F2

g. Menjumlahkan hasil akhir a, b, c, d, e, f, g, h dengan inisial *hash value* $H^{(i)}$

$H_0^{(i)}$	$= a + H_0^{(i)}$
$H_1^{(i)}$	$= b + H_1^{(i)}$
$H_2^{(i)}$	$= c + H_2^{(i)}$
$H_3^{(i)}$	$= d + H_3^{(i)}$
$H_4^{(i)}$	$= e + H_4^{(i)}$
$H_5^{(i)}$	$= f + H_5^{(i)}$
$H_6^{(i)}$	$= g + H_6^{(i)}$
$H_7^{(i)}$	$= h + H_7^{(i)}$

h. *Output*

Setelah mengulangi langkah 1 hingga 4 sebanyak N kali, fungsi *hash* yang dihasilkan adalah sebagai berikut :

$$H_0^{(N)} || H_1^{(N)} || H_2^{(N)} || H_3^{(N)} || H_4^{(N)} || H_5^{(N)} || H_6^{(N)} || H_7^{(N)}$$

2.8 Ganache

Ganache sebelumnya dikenal sebagai *Testrpc* dan hadir dalam bentuk baris perintah dan UI. *Ganache* merupakan sebuah *blockchain* virtual yang mempunyai sepuluh alamat *Ethereum* standar dengan kunci pribadi yang memuatnya terlebih dahulu dengan simulasi masing-masing mempunyai 100

- Hak Cipta Dilindungi Undang-Undang**
- Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 - Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Ether untuk menguji *smart contract* pada *blockchain* lokal. Dengan *ganache* tidak ada penambangan melainkan secara otomatis mengonfirmasi setiap transaksi. Sangat nyaman untuk sistem operasi seperti *windows*, *linux* dan *mac*. (Khan, Arshad, Mushtaq, Khalique, & Husein, 2020)

Ganache adalah kerangka kerja yang disediakan oleh *truffle* dan digunakan sebagai *blockchain* lokal untuk pengembangan *Ethereum* oleh pengembang yang digunakan untuk menerapkan *smart contract*, membuat aplikasi, dan melakukan pengujian. *Ganache* membuat server lokal serta akun dengan kunci pribadi. (Gupta, Jha, Shukla, Raj, & Sultana, 2020)

2.9 Truffle Framework

Truffle adalah alat yang ampuh untuk bekerja dengan *smart contract ethereum*. Ini digunakan untuk kompilasi, penyebaran dan penautan *smart contract*, menyediakan platform pengujian untuk kontrak otomatis, mengelola jaringan dan paket. (Khan, Arshad, Mushtaq, Khalique, & Husein, 2020)

Truffle membantu dalam menyusun *smart contract* yang dibangun menggunakan bahasa *solidity* dan yang memiliki logika bisnis di dalamnya dan menerapkan kontrak tersebut ke jaringan *Ethereum* lokal. Kontrak ini dapat diakses oleh semua sistem di jaringan lokal. Setiap *node* dapat melakukan transaksi jika memenuhi aturan kontrak. Setelah kontrak diterapkan di jaringan, ini memungkinkan pengguna untuk berinteraksi dengannya dan melakukan transaksi untuk membawa perubahan dalam status kontrak. (Gupta, Jha, Shukla, Raj, & Sultana, 2020)

2.10 Matemask

Matemask merupakan aplikasi yang dipasang pada *browser* untuk memudahkan pengguna dalam berinteraksi dengan sistem berbasis *Blockchain Ethereum*. Selain itu juga *Metamask* dapat digunakan untuk melakukan konfirmasi transaksi seperti yang telah diterapkan pada sistem ini. (Badawi)

Metamask membantu menghubungkan aplikasi web terdesentralisasi untuk terhubung ke jaringan *Ethereum* lokal dan juga memberikan dompet yang dibutuhkan untuk transaksi. Pertama akun diatur di *metamask* oleh akun yang disediakan oleh *ganache* yang memberi anda sepuluh akun, setiap akun memiliki

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

kunci pribadi yang digunakan untuk mengatur akun di *metamask*. Sekarang ketika masuk ke aplikasi web melalui browser web di mesin, akun *metamask* dipilih dan kemudian dapat melakukan transaksi menggunakan akun itu. (Gupta, Jha, Shukla, Raj, & Sultana, 2020)

Beberapa fitur utama *metamask* dibahas sebagai berikut (Jyoti & Chauhan, 2020):

1. *Metamask* memungkinkan untuk membuat akun di beberapa jaringan *Ethereum*.
2. Kunci pribadi untuk akun memungkinkan untuk mengimpornya atau mengekspor akun baru.
3. Dompot memungkinkan untuk beralih ke beberapa jaringan *Ethereum*, dan dengan demikian akun saldo saat ini tercermin untuk setiap jaringan.
4. Transaksi dilakukan antar akun dan memungkinkan untuk menukar Eter dari satu akun ke akun lainnya.
5. Akun *Metamask* ditambahkan dengan token dan juga transaksi mendalam pada penjelajah rantai blok, *Etherscan* juga dicatat.

2.11 *NPM (Node Package Manager)*

NPM adalah manajer paket yang mengelola, menginstal, memperbarui atau menghapus paket *node.js* dalam sebuah aplikasi. Ini adalah alat berbasis baris perintah. *NPM* beroperasi dalam dua mode yaitu mode lokal dan mode global. Dalam mode global, semua aplikasi *node.js* terpengaruh. Sedangkan dalam mode lokal hanya direktori tertentu dari aplikasi yang terpengaruh. (Khan, Arshad, Mushtaq, Khaliq, & Husein, 2020)

Node js digunakan untuk memberikan *GUI* untuk berkomunikasi dengan *smart contract* yang telah diterapkan. Untuk melakukan ini dengan cara menggunakan *library Web3*. *Web3* adalah *Ethereum JavaScript API* yang menggunakan koneksi *HTTP* memungkinkan kita untuk terhubung ke *node Ethereum* lokal atau jarak jauh. (Gupta, Jha, Shukla, Raj, & Sultana, 2020)

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

2.12 Penelitian Terkait

Penelitian terkait yang telah dilakukan dijelaskan pada table dibawah ini. Table tersebut berisikan judul penelitian, penulis yang melakukan penelitian, dan hasil dari penelitian tersebut.

Table 2. 3 Penelitian Terkait

No	Judul	Penulis	Hasil
1.	<i>Smart Contract Blockchain pada E-Voting</i>	Teresa Enades Hari Setia, Ajib Susanto	Pemungutan suara elektronik berbasis teknologi blockchain bisa menjadi tempat yang sangat aman untuk menyimpan data pemungutan suara. Dengan menggunakan kontrak pintar dengan bahasa pemrograman Solidity untuk pengujian, tidak ada yang dapat melakukan operasi dan pemilihan beberapa kali. Dengan cara ini, teknologi blockchain dalam pemungutan suara elektronik tidak mudah dibobol, karena setiap pemilih memiliki alamat blockchain uniknya sendiri, yang tidak dapat digunakan kembali. Dalam penelitian ini, mereka masih menggunakan situs remix Ethereum untuk membuat kode untuk melakukan transaksi.
2.	<i>Aplikasi Voting Online dengan Menggunakan Teknologi Blockchain</i>	Ahmad Fajar Prasetyo, Dr. Ir. Rinaldi Munir, M.T.	Hasil pada <i>blockchain</i> tidak dapat diganti karena masih dalam <i>chipertext</i> . Setelah semua hasil dari <i>blockchain</i> terkumpul dilakukan deskripsi untuk mengetahui hasil <i>voting</i> . Deskripsi dilakukan dengan menggunakan semua kunci privat yang telah tersebar ke

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

			<i>stakeholder.</i>
3.	Implementasi <i>Blockchain</i> : Studi Kasus <i>e-Voting</i>	Satria Damai Kurnia Hu, Henry Novianus Palit, Andreas Handojo	Sistem pemungutan suara elektronik yang tidak memakai <i>blockchain</i> akan memberi definisi sendiri mengenai <i>ballot</i> yang dikatakan valid oleh pembuat sistem. Pemberian definisi pastinya akan hanya bergantung dengan kemampuan sistem yang dibuat dan hanya dapat divalidasi kebenarannya oleh sistem tersebut. Sehingga bila sistem tersebut mengalami masalah, <i>ballot</i> yang dikatakan valid dapat berubah. Sedangkan sistem <i>e-Voting</i> dengan <i>blockchain</i> , pemberian definisi <i>ballot</i> yang valid melibatkan program dari luar sistem tersebut yaitu <i>blockchain</i> . Sehingga bila sistem mengalami masalah, <i>ballot</i> yang dikatakan valid tidak akan berubah dan validasi tetap dapat dilakukan oleh <i>blockchain</i> .
4.	Implementation of <i>Smart Contracts</i> Ethereum <i>Blockchain</i> in <i>Web-Based Electronic Voting</i> (e-voting)	Faiq Dzulfikar, Ajib Susanto	Dari perancangan dan implementasi sistem e-voting yang berbasis pada <i>Ethereum Blockchain</i> , dapat ditarik kesimpulan diantaranya: 1) Sistem e-voting berbasis <i>Ethereum Blockchain</i> dapat berjalan dengan baik. 2) Sistem e-voting ini mampu memvalidasi identitas pemilih dengan baik dan mencegah pemilu terulang. 3) Sistem e-voting ini dapat menyimpan data dengan aman dan terpercaya. 4) Dengan menggunakan sistem pemilu ini, proses pemungutan suara akan

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

			jauh lebih cepat dan aman. 5) Proses pemungutan suara dan penghitungan jumlah suara akan lebih cepat karena proses pemungutan suara dilakukan secara real-time.
5.	<i>Secure Digital Voting System based on Blockchain Technology</i>	Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan	jurnal ini menyajikan upaya untuk memanfaatkan manfaat blockchain seperti fondasi kriptografi dan transparansi untuk mencapai skema yang efektif untuk evoting. Skema yang diusulkan sesuai dengan persyaratan fundamental untuk skema e-voting dan mencapai verifikasi ujung ke ujung. jurnal ini menyajikan rincian skema e-voting yang diusulkan beserta implementasinya menggunakan platform <i>Multichain</i> . jurnal ini menyajikan evaluasi mendalam tentang skema yang berhasil menunjukkan keefektifannya untuk mencapai skema e-voting yang dapat diverifikasi secara end-to-end.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

BAB III METODOLOGI PENELITIAN

Metodologi penelitian adalah rangkaian tahapan yang disusun secara sistematis yang dijadikan pedoman pelaksanaan penelitian untuk mencapai tujuan dari penelitian. Berikut rangkaian yang akan dilakukan pada penelitian ini yaitu sebagai berikut:



Gambar 3. 1 Flowchart Metodologi Penelitian

3.1 Perumusan Masalah

Setelah melakukan identifikasi masalah diatas, disimpulkan bahwa penyelesaian dari permasalahan yang ada pada penelitian adalah

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

mengimplementasikan teknologi *blockchain* menggunakan *smart contract* pada *e-voting*.

3.2 Studi Pustaka

Studi Pustaka adalah melakukan review pada jurnal, buku dan lainnya untuk memahami yang menjadi kebutuhan dalam mengimplementasikan *blockchain* menggunakan *smart contract* pada *E-Voting*.

3.3 Analisa

Tujuan dari adanya analisis kebutuhan sistem adalah untuk mengetahui kebutuhan sistem yang nantinya dapat digunakan dalam tahap perancangan sistem. Adapun metode analisis terhadap kebutuhan sistem ini diantaranya adalah :

1. Analisis proses bisnis yaitu cara yang dipakai untuk mengetahui Langkah dalam proses sistem yang terjadi.
2. Desain arsitekur yaitu berupa desain arsitektur sistem, desain uml activity, desain uml sequence.

3.4 Perancangan

Pada bagian perancangan ini merupakan tahap perancangan sistem yaitu perancangan antarmuka sistem berdasarkan kebutuhan untuk bisa mengimplementasikan teknologi *blockchain* menggunakan *smart contract* pada *e-voting*.

3.5 Implementasi dan Pengujian

3.5.1 Implementasi

Pada tahapan implementasi ini merupakan tahapan yang dilakukan oleh peneliti setelah Analisa dan perancangan selesai. Implementasi adalah tahapan dalam membuat dan menyusun perangkat lunak dengan Bahasa pemrograman. Bahasa pemrograman yang digunakan adalah *Solidity* dengan menggunakan *Ganache* sebagai *blockchain* lokal sebagai database terdesentralisasi.

3.5.2 Pengujian

Pengujian merupakan tahap terakhir dalam tahapan penelitian. Pada tahap ini, terdapat dua jenis pengujian yang dilakukan yaitu:

- 1) Pengujian unit testing *smart contract*.



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Pengujian ini dilakukan sebelum smart contract di deploy ke *blockchain* untuk melakukan tes terhadap setiap unit fungsi pada *smart contract*.

- 2) Pengujian fungsionalitas sistem.

Pengujian ini dilakukan untuk mengetahui apakah sistem berjalan dengan baik dan sesuai dengan yang di inginkan.

- 3) Pengujian *smart contract cost*.

Pengujian ini dilakukan untuk mengetahui besaran biaya transaksi yang digunakan ketika pengguna mengeksekusi sebuah fungsi *smart contract* yang terintegrasi dengan *blockchain Ethereum*. Berikut ini adalah mencari biaya dari satuan gas ke ether atau rupiah.

$$Cost = gas\ used \times gas\ price \times ether\ price \tag{3.1}$$

- cost* = biaya yang dikeluarkan
- gas used* = gas yang terpakai (gas)
- gas price* = harga gas dalam ether (ether)
- ether price* = harga *Ethereum* (ether)

3.6 Kesimpulan dan Saran

Tahap kesimpulan dan saran ini adalah tahap terakhir dari penelitian ini. Pengambilan kesimpulan berisikan tentang keberhasilan terhadap mengimplementasikan teknologi *blockchain* menggunakan *smart contract* pada *e-voting* apakah sudah sesuai dengan yang diharapkan serta dapat dioperasikan dengan baik. Serta terdapat saran-saran yang membangun terhadap penelitian ini agar memunculkan penelitian baru yang dapat memperbaiki penelitian sebelumnya.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

BAB IV ANALISA DAN PERANCANGAN

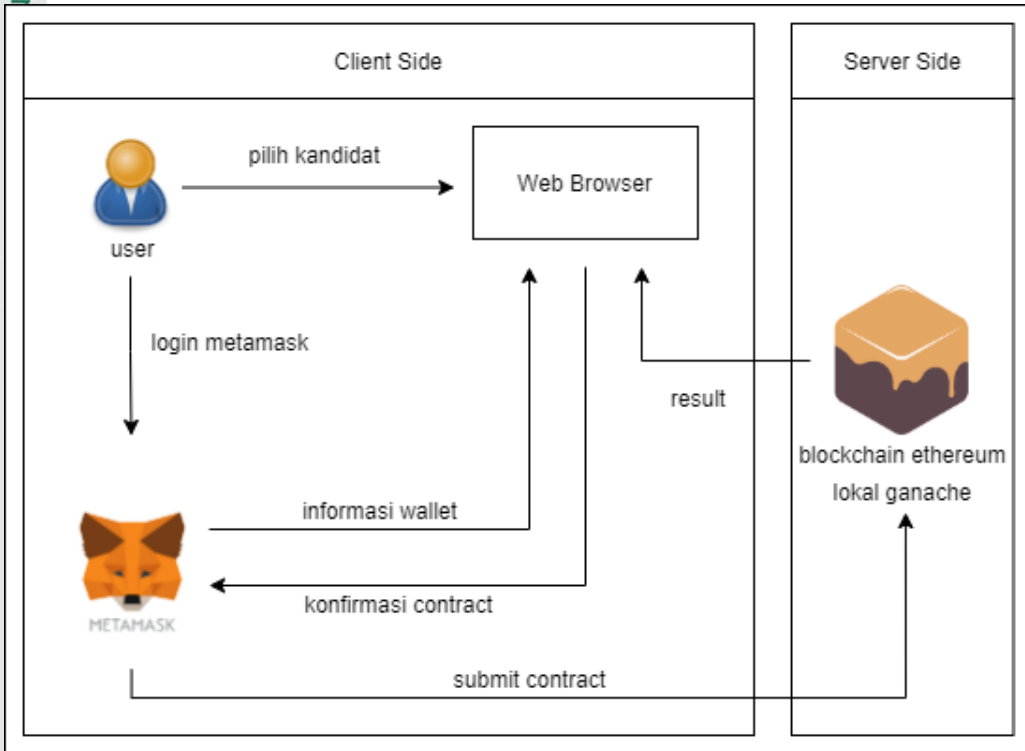
4.1 Analisis Proses Bisnis

Analisis proses bisnis adalah suatu cara atau metode yang digunakan untuk mengetahui urutan Langkah dalam pelaksanaan di suatu organisasi untuk mendapatkan hasil akhir yang sesuai dan terukur. Analisis proses bisnis pada penelitian ini adalah sebagai berikut:

1. Sistem melakukan *set* sebagai admin untuk *user* atau *account address* yang pertama masuk ke sistem.
2. Sistem dapat menambah data kandidat yang hanya dilakukan oleh admin saja.
3. Sistem dapat memulai dan mengakhiri *voting* yang hanya bisa dilakukan oleh admin saja
4. *Voter* pada sistem ini dibuat dengan cara melakukan *import mnemonic* dari *blockchain ethereum* lokal *ganache* ke *metamask* untuk bertransaksi antara *user* dengan *blockchain ethereum*.
5. Sistem dapat melakukan *voting* yang dilakukan oleh semua *user* atau *account address* pada *metamask*.
6. Setiap transaksi dengan *blockchain ethereum* lokal *ganache* terjadi, maka *metamask* meminta konfirmasi dengan membaca *account address* yang melakukan transaksi.

4.2 Desain Arsitektur

Desain arsitektur dihasilkan berdasarkan analisis dari studi Pustaka yang sebelumnya telah dilakukan, yang mana dalam mengimplementasikan teknologi *blockchain* menggunakan *smart contract* pada e-voting membutuhkan penyesuaian berbagai hal dalam kebutuhan sistem. Untuk terkoneksi ke dalam sistem berbasis *smart contract blockchain ethereum*, maka dibutuhkan tersambung pada *metamask* yang berguna untuk terhubung dengan *blockchain ethereum* lokal yaitu *ganache*.



Gambar 4. 1 Desain Arsitektur Sistem

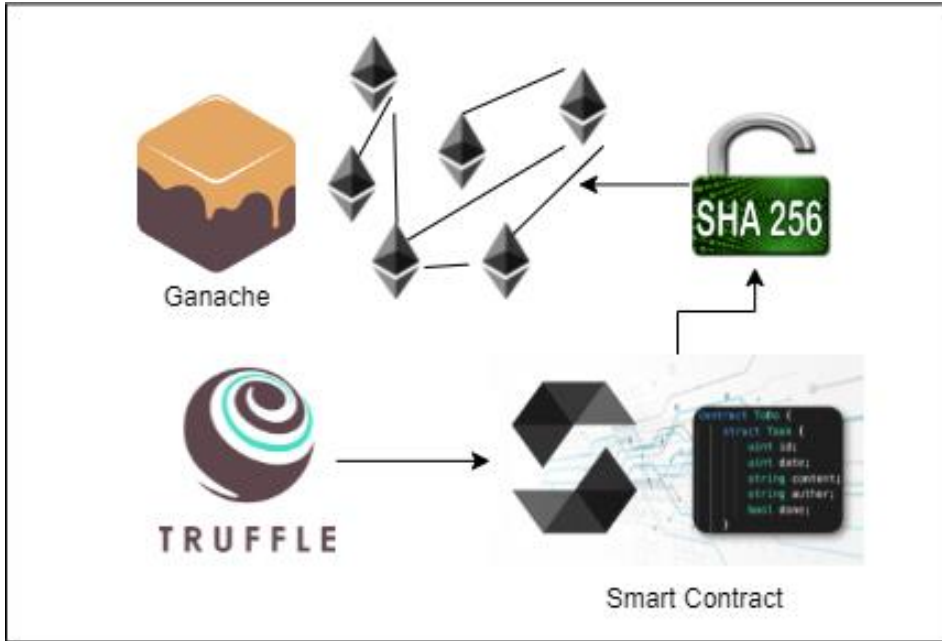
Pada gambar 4.1 dijelaskan bahwa untuk dapat melakukan transaksi dengan sistem maka harus login *metamask* terlebih dahulu dan *metamask* akan memberikan informasi *wallet* kepada *user* dan juga bisa melakukan konfirmasi dan *submit contract* ke dalam jaringan *blockchain Ethereum* lokal *ganache*. *Blockchain ethereum* lokal *ganache* akan memberikan *result* ke *user*.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

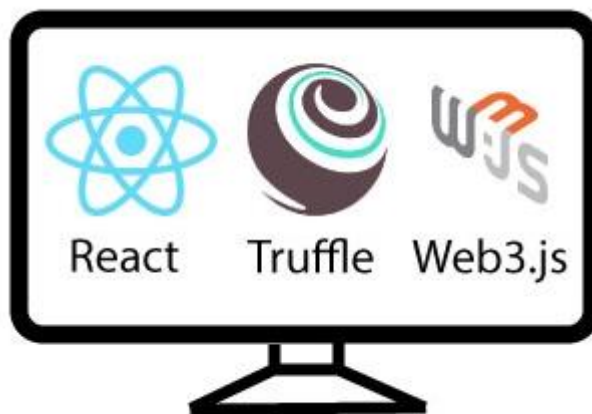
Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Gambar 4. 2 Smart Contract Development pada Private Testnet

Pada gambar 4.2. dijelaskan bahwa untuk membuat sebuah sistem berbasis *blockchain* maka diperlukan *truffle framework* untuk membuat *smart contract* menggunakan bahasa *solidity* yang mana *blockchain ethereum* akan menyimpan transaksi dalam bentuk kriptografi *sha-256*. Pada pengembangan *smart contract* ini dilakukan pada *blockchain ethereum* lokal yang disebut sebagai jaringan *private testnet*.



Gambar 4. 3 Platform Web

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Pada gambar 4.3. merupakan sebuah *platform* web yang dibuat untuk mempermudah *user* untuk berinteraksi dengan sistem yang dibangun menggunakan *javascript framework* yaitu *react js* untuk tampilan dan *trauffle framework* untuk membuat *smart contract*, sedangkan *web3 js* merupakan sebuah *ethereum javascript API* yang digunakan untuk menghubungkan antara tampilan dengan *smart contract*.

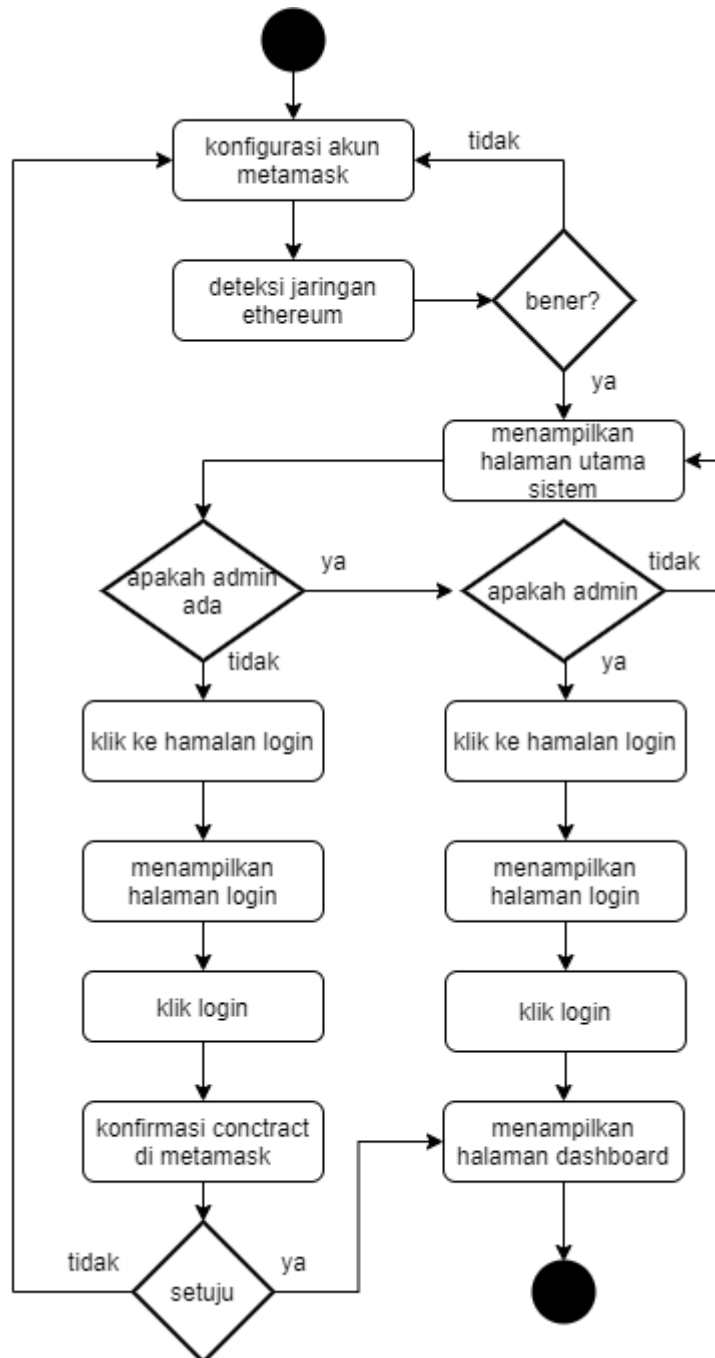
4.2.2 Desain UML Activity Diagram

Pada *activity* Diagram ini menggambarkan aktivitas *user* beserta proses bisnis dari awal sampai selesai. Berikut ini adalah diagram proses login ditampilkan pada Gambar 4.2.



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



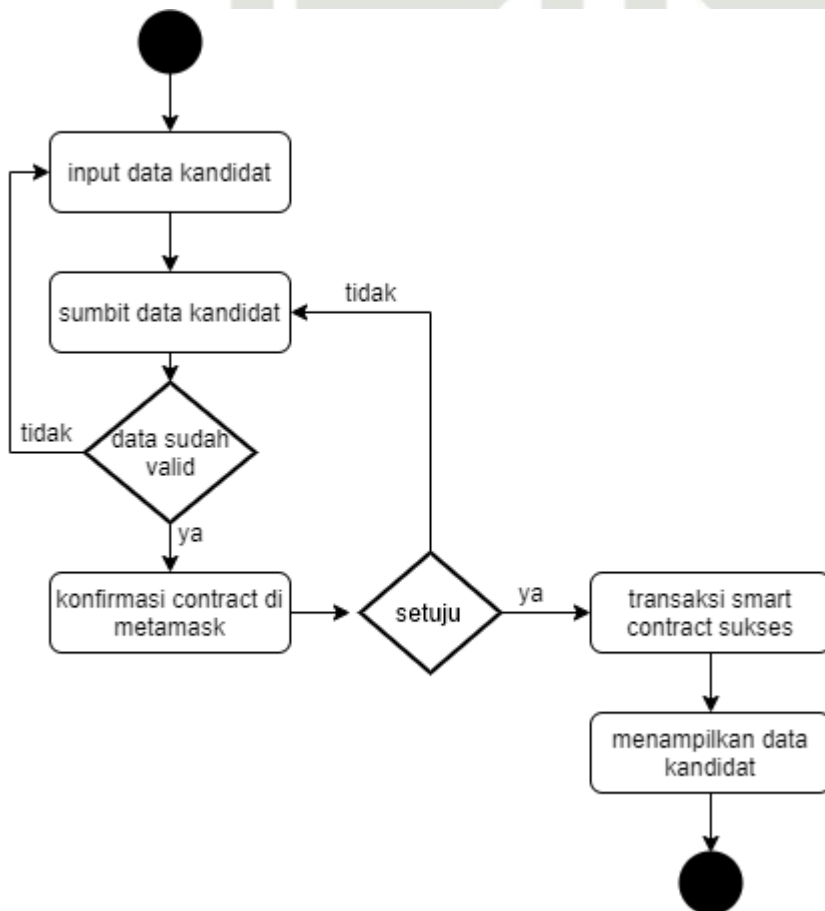
Gambar 4. 4 Activity Diagram Proses Login Admin

Activity diagram pada Gambar 4.2 merupakan proses login. Proses login ini hanya bisa dilakukan oleh admin, Langkah pertama diawali dengan sistem menampilkan halaman utama dan mengecek apakah admin sudah ada di dalam *blockchain ethereum* lokal *ganache*, apabila ada maka di cek lagi apakah *account*

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

address itu adalah admin, apabila admin dapat login ke dashboard admin, apabila bukan admin, maka *account address* tersebut tidak bisa ke halaman dashboard admin, apabila belum ada admin yang di *set* sebelumnya, maka *account address* tersebut bisa ke halaman login dan melakukan konfirmasi *smart contract* ke *blockchain ethereum* lokal *ganache* dan setelah data *account address* tersebut di *set* menjadi admin, maka bisa mengakses halaman dashboard admin. Pada halaman dashboard admin bisa menginput data kandidat. Berikut ini adalah Diagram proses input data kandidat yang ditampilkan pada Gambar 4.3.



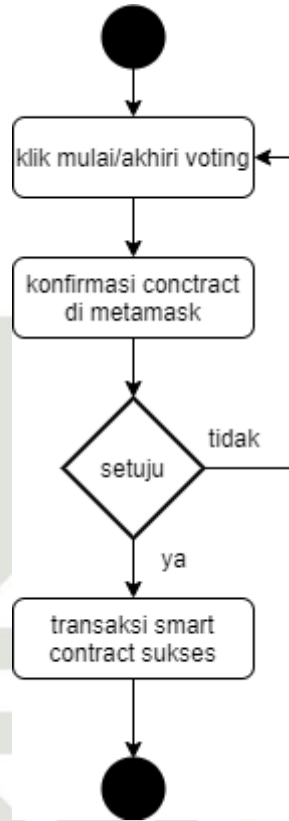
Gambar 4. 5 Activity Diagram Input Data Kandidat

Setelah admin login ke halaman dashboard, maka Langkah selanjutnya adalah input data kandidat yang dilakukan oleh admin dan saat submit data maka *metamask* memberikan konfirmasi *smart contract* untuk data bisa masuk ke *blockchain ethereum* lokal *ganache* seperti Gambar 4.3. setelah semua data

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

kandidat telah di masukkan ke dalam *blockchain ethereum* lokal *ganache*, maka admin akan memulai *voting* yang ditampilkan pada Gambar 4.4.

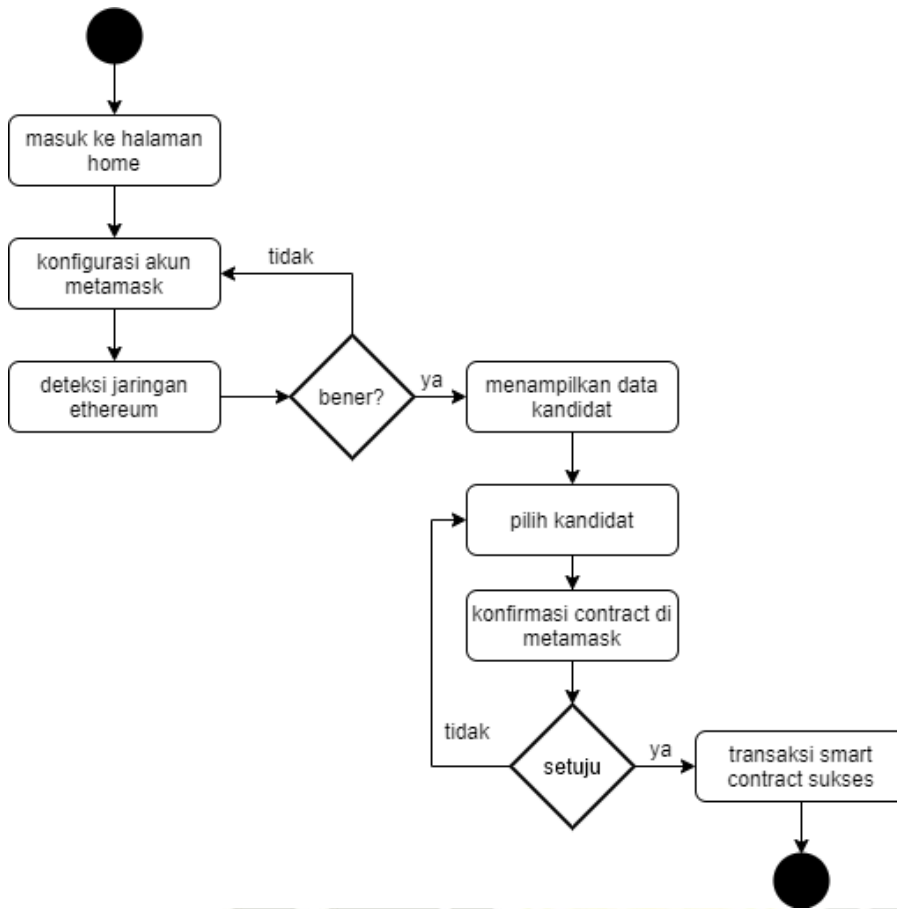


Gambar 4. 6 Activity Diagram Mulai/Akhiri Voting

Pada gambar 4.4 merupakan proses memulai atau mengakhiri voting yang dilakukan hanya oleh admin saja. Admin mengklik tombol mulai/akhiri voting dan *metamask* akan menampilkan konfirmasi *smart contract* agar data tersebut masuk ke *blockchin ethereum* lokal *ganache*. setelah admin memulai *voting* maka *users* bisa melakukan *voting* yang terdapat pada gambar 4.5.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Gambar 4. 7 Activity Diagram Proses Melakukan Voting

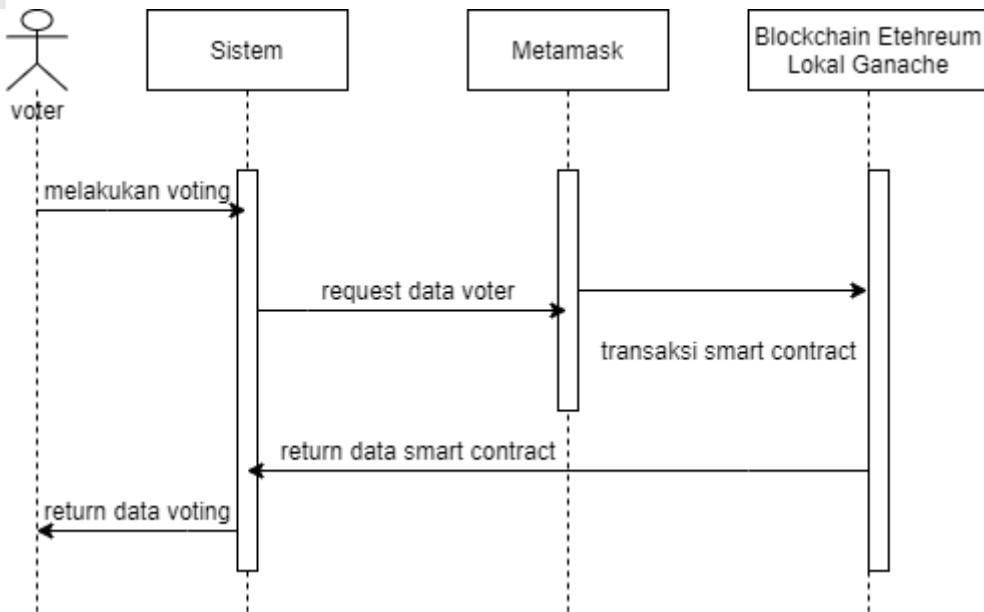
Pada Gambar 4.5 merupakan proses *voter* melakukan *voting* dan hanya bisa dilakukan sekali oleh satu *account address* pada *metamask*. Sebelum *voter* melakukan *voting*, maka melakukan konfigurasi *metamask* terlebih dahulu dan barulah setelah itu *voter* melakukan *voting*, dan apabila transaksi benar maka sistem akan memberitahu bahwa transaksi ke *blockchain Ethereum* lokal *ganache* sukses.

4.2.3 Desain UML Sequence Diagram

Sequence diagram menggambarkan bagaimana entitas dan sistem akan saling berinteraksi dan juga menggambarkan perilaku dalam suatu scenario. Untuk itu maka dibuatlah dalam sebuah model *sequence diagram*. Berikut adalah *sequence diagram* sistem yang ditampilkan pada Gambar 4.5.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Gambar 4. 8 Sequence Diagram Sistem

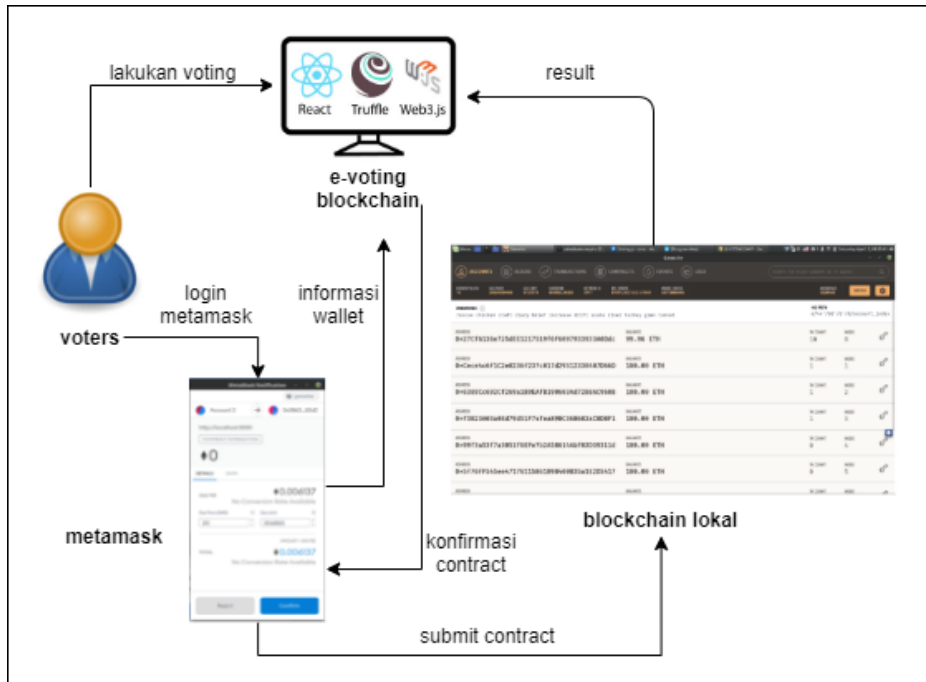
Pada gambar 4.6 tersebut memiliki 1 aktor dan objek yaitu sistem, metamask, dan blockchain ethereum lokal yaitu ganache. Proses pada sequence diagram tersebut diawali dengan voter melakukan voting dan setelah itu melakukan request data akun pada metamask lalu terjadilah transaksi smart contract ke blockchain ethereum lokal yaitu ganache dan hasilnya yang berupa data smart contract dikembalikan ke sistem.

4.3 Mekanisme E-Voting Blockchain

Mekanisme e-voting berbasis blockchain dijelaskan pada gambar dibawah

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Gambar 4. 9 Mekanisme E-Voting Blockchain

Pada gambar 4.9. dijelaskan mekanisme *e-voting* bahwa *voters* harus login *metamask* terlebih dahulu dengan cara memasukkan *private key* pada salah satu akun pada *ganache* atau langsung *import* seluruh akun dengan cara memasukkan *mnemonic*. Setelah itu *voters* bisa melakukan *voting* dan *metamask* menampilkan informasi biaya yang akan digunakan berupa gas dan meminta konfirmasi *contract* setelah kita memilih kandidat. Apabila *contract* dikonfirmasi maka data *voting* akan tersimpan ke *blockchain* lokal yaitu *ganache* dan apabila *voters* ingin melakukan pemilihan lebih dari satu kali, maka tidak bisa karena *contract* diawal tidak memperbolehkan memilih lebih dari satu kali. Dan hasil *voting* yang tersimpan dalam *blockchain* lokal akan ditampilkan ke sistem untuk dilihat oleh *voters*.

4.4 Perancangan Antarmuka

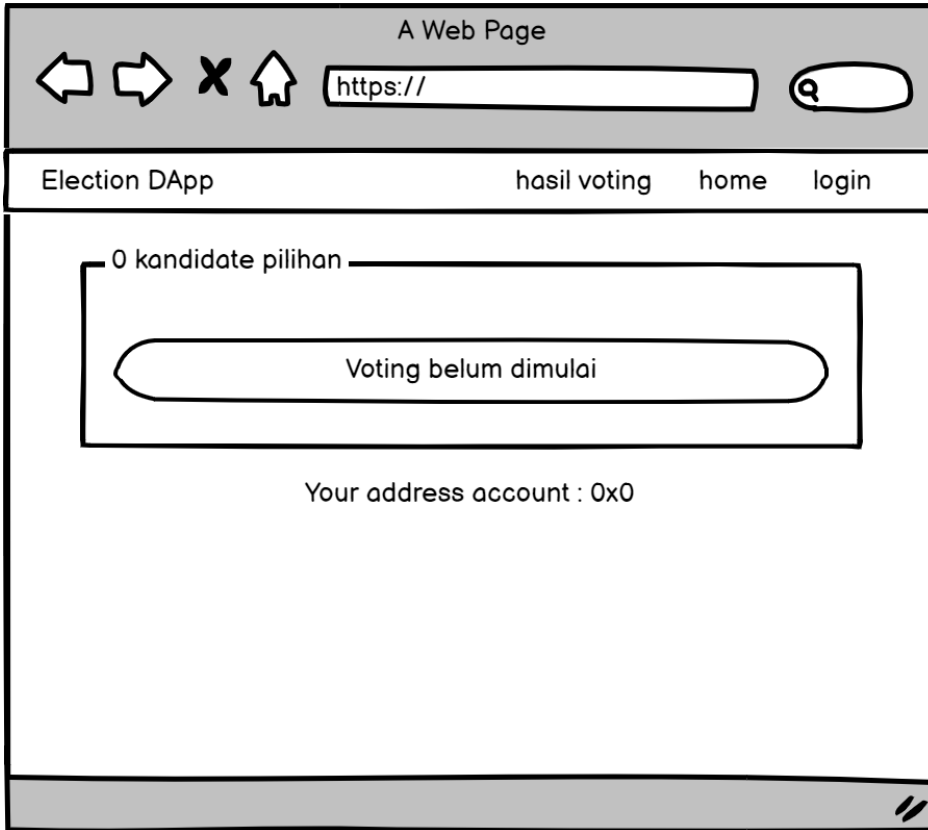
Antarmuka adalah sarana untuk memudahkan *user* berinteraksi dengan sistem. Perancangan antarmuka pada sistem ini dibuat menggunakan *balsamiq cloud*. Terdapat 7 antarmuka pada sistem ini yang mempunyai fungsi dari masing-masing antarmuka.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

4.4.1 Halaman Awal Sistem

Halaman awal sistem ini menampilkan sebuah *address account*, tombol login untuk admin.



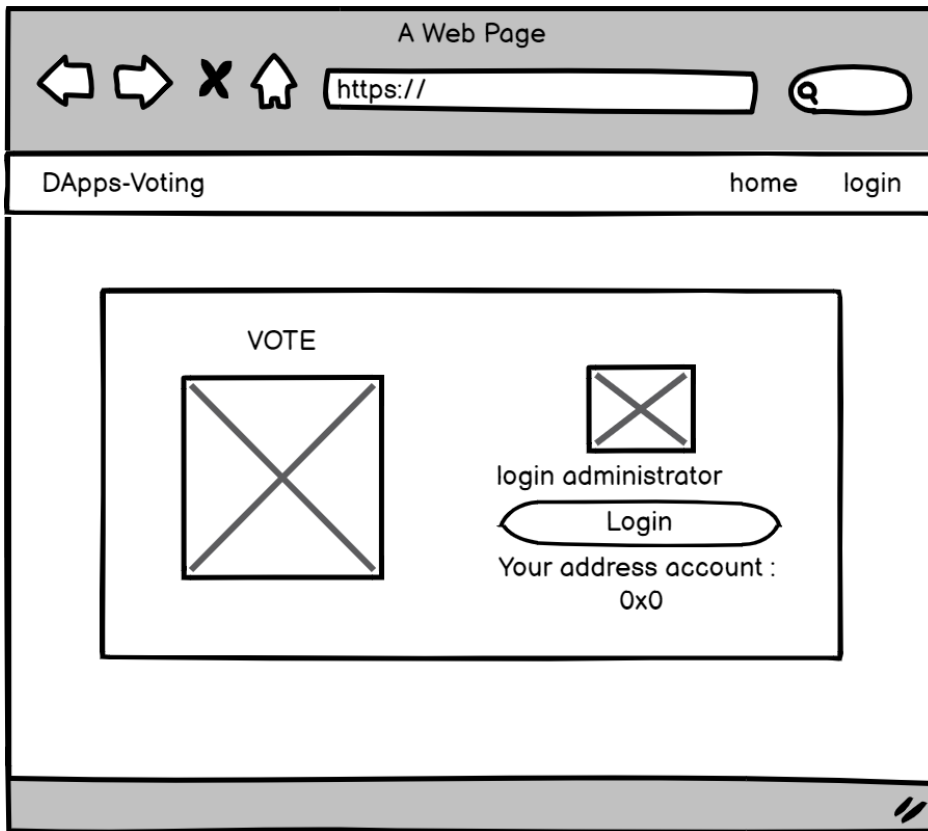
Gambar 4. 10 Halaman Awal Sistem

4.4.2 Halaman Login Admin

Halaman *login* admin ini hanya terdapat tombol untuk *login*, apabila *address account* yang terkonfigurasi sama dengan *address account* admin di *blockchain Ethereum* maka bisa login ke *dashboard* admin.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



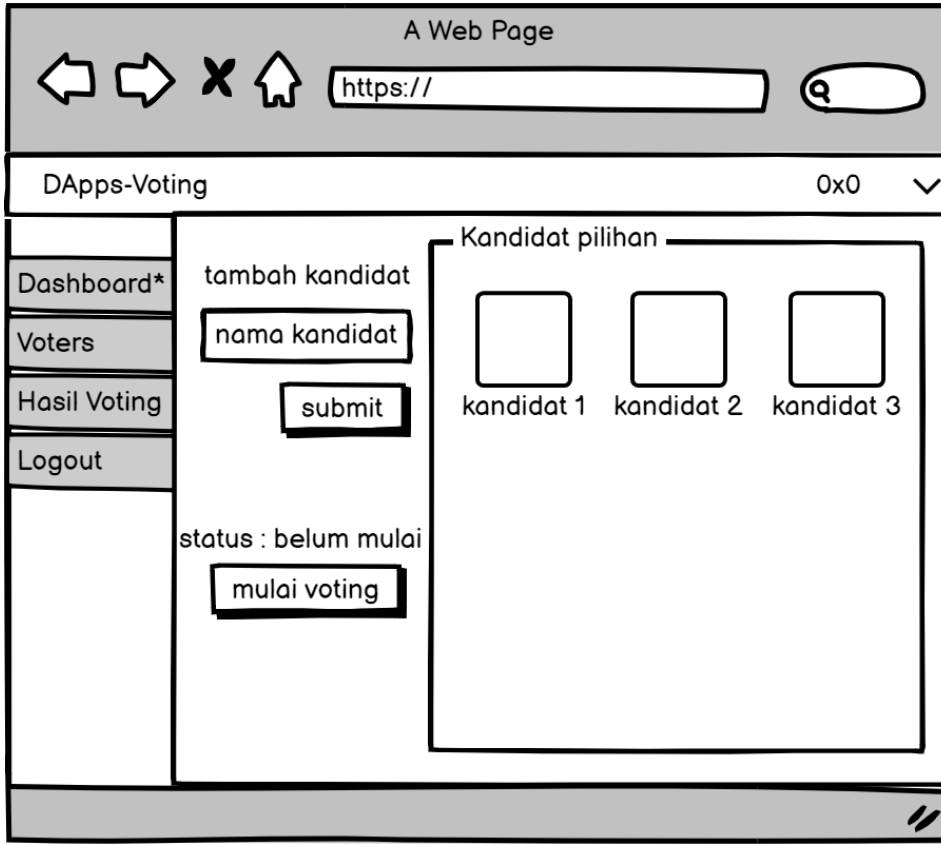
Gambar 4. 11 Halaman Login Admin

4.4.3 Halaman Dashboard Admin

Halaman *dashboard* admin ini menampilkan *form* untuk tambah data kandidat dan juga menampilkan data-data kandidat yang telah ditambahkan. Selain itu juga menampilkan tombol untuk memulai *voting*.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



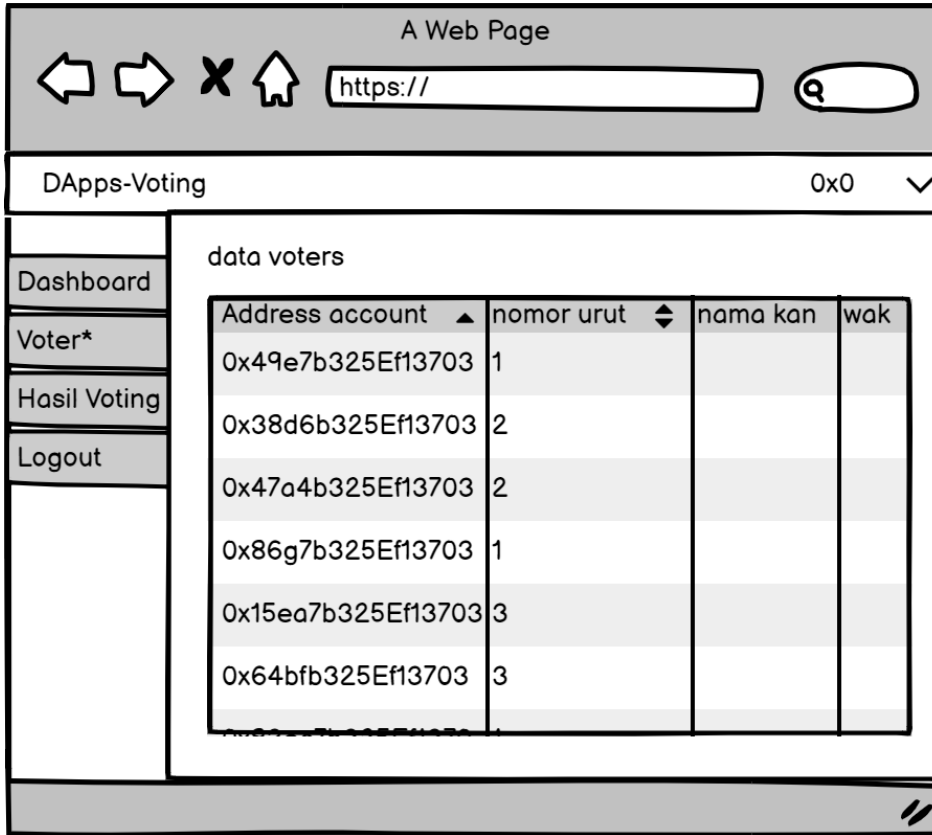
Gambar 4. 12 Halaman Dashboard Admin

4.4.4 Halaman Data Voters

Halaman data *voters* ini menampilkan data *voters* yang telah melakukan voting.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



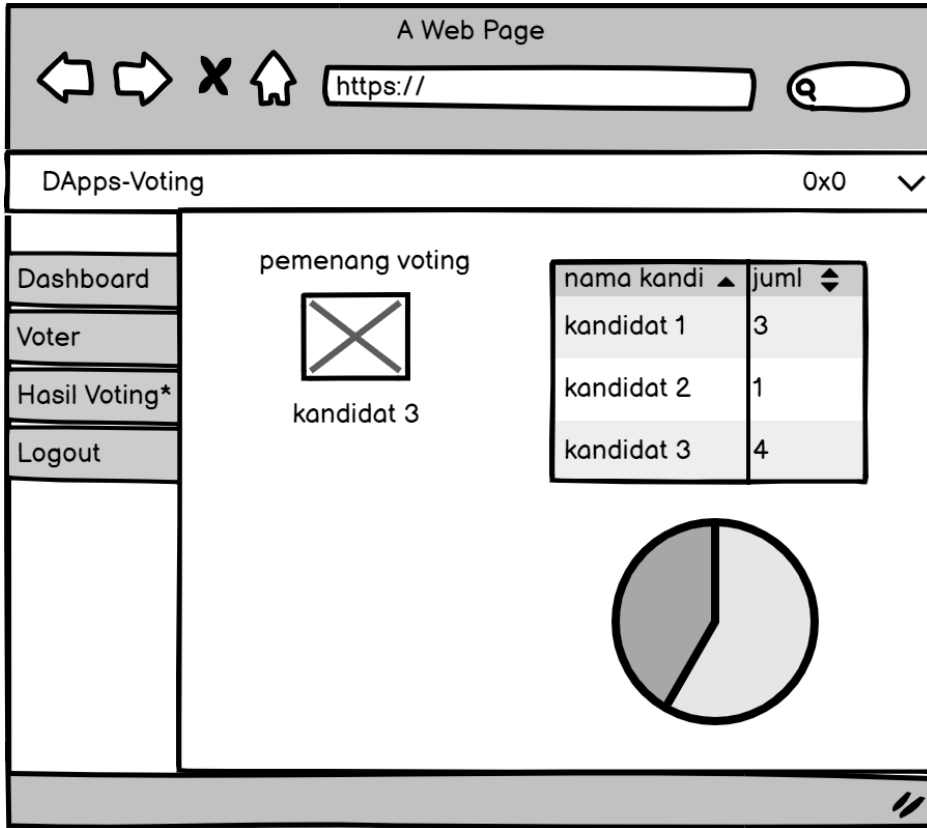
Gambar 4. 13 Halaman Data Voter

4.4.5 Halaman Admin Hasil Voting

Halaman admin hasil voting ini menampilkan pemenang voting dan data suara yang dimiliki setiap kandidat dalam bentuk table dan *pie chart*.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



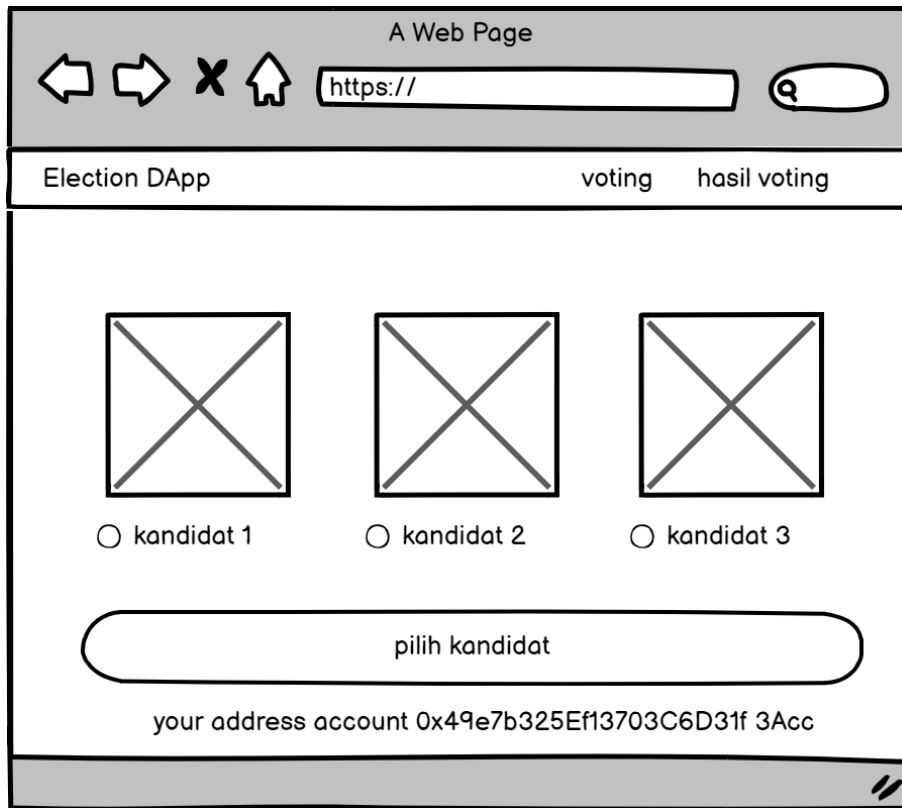
Gambar 4. 14 Halaman Admin Hasil Voting

4.4.6 Halaman Awal Voter

Halaman awal *voters* ini menampilkan data-data kandidat yang akan dipilih pada voting dengan melakukan klik radio button kandidat yang dipilih lalu mengklik tombol pilih kandidat.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



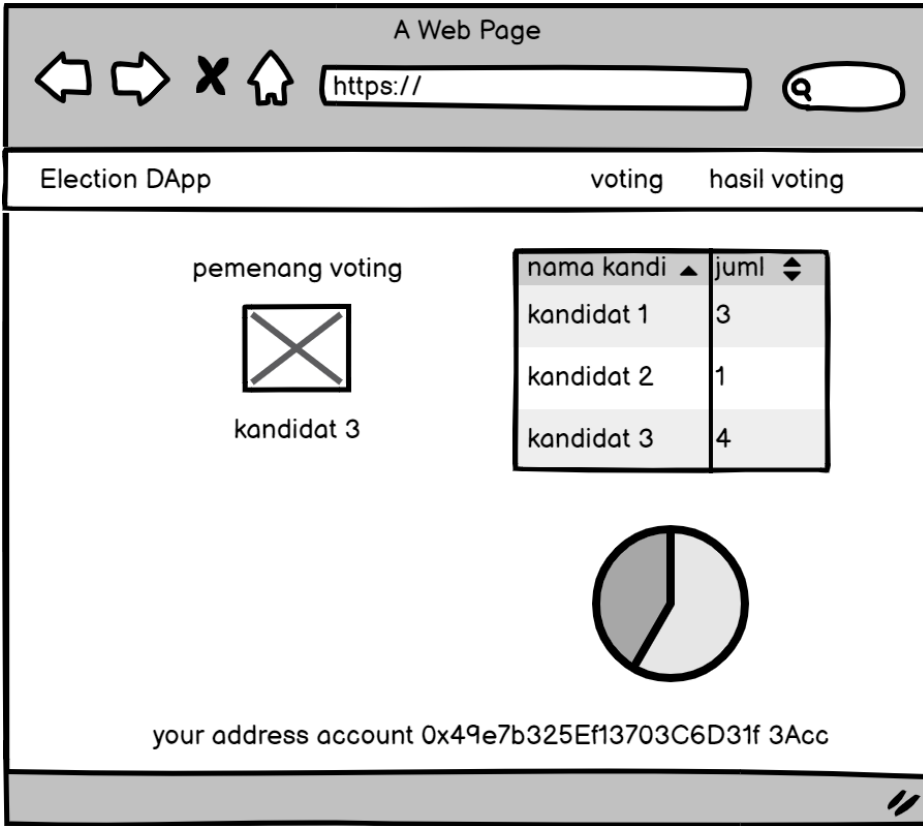
Gambar 4. 15 Halaman Awal Voter

4.4.7 Halaman Hasil Voting

Halaman hasil voting ini untuk *voter* yang menampilkan kandidat yang dipilih dan menampilkan pemenang *voting* beserta jumlah suara yang diperoleh oleh setiap kandidat dalam bentuk tabel dan *pie chart*.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Gambar 4. 16 Halaman Hasil Voting

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

BAB VI PENUTUP

6.1 Kesimpulan

Pada penelitian ini ditarik kesimpulan sebagai berikut:

1. Implementasi teknologi *blockchain* menggunakan *smart contract* pada studi kasus *e-voting* berhasil di selesaikan.
2. Pada penelitian ini masih menggunakan *blockchain Ethereum* lokal yaitu *ganache*.
3. Sistem ini hanya untuk implementasi integritas data menggunakan *blockchain ethereum*.
4. Hasil dari pengujian *unit testing* pada *smart contract* berjalan dengan baik dan normal.
5. Hasil dari pengujian fungsionalitas sistem, bahwa sistem berjalan dengan baik dan normal.
6. Biaya pada *smart contract* hanya dihitung pada transaksi di *blockchain ethereum* lokal *ganache* saja.
7. Hasil dari pengujian biaya *smart contract*, maka didapat biaya paling tinggi dari beberapa transaksi yaitu transaksi melakukan *voting* dengan biaya Rp. 16.503,42.

6.2 Saran

Pada penelitian ini ada beberapa saran untuk mengembangkan teknologi *blockchain* menggunakan *smart contract* pada studi kasus *e-voting*, diantaranya adalah:

1. Membangun sistem web *e-voting* berbasis *blockchain ethereum* dengan fitur sistem yang lebih lengkap untuk mencari biaya transaksi *smart contract* pada jaringan *ethereum*.
2. Membangun sistem *e-voting* berbasis web dengan menambahkan autentikasi *user* dengan KTP berbasis *blockchain ethereum*.
3. Membangun sistem *e-voting smart contract Ethereum* berbasis *mobile*.

DAFTAR PUSTAKA

- Alvaro , D. (2018). Implementasi Blockchain untuk Distribusi Kunci Publik Terdesentralisasi.
- Amelia, R., Bahri, S., & Sanjaya, W. (2018). PERANCANGAN APLIKASI E-VOTE BERBASIS MOBILE ANDROID PADA PEMILIHAN KETUA RT NGESTIHARJO RT 02/15 SISWODIPURAN BOYOLALI. *Journal Informatic Technology And Communication*, 2-4.
- Aprialim, F., Adnan, & Paundu, A. W. (2017). Penerapan Blockchain dengan Integrasi Smart Contract pada Sistem Crowdfunding. *JURNAL RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 149.
- Ardilla , R. (2018). RANCANG BANGUN SISTEM E – VOTING DENGAN METODE ENKRIPSI BLOCKCHAIN DI KOTA MOJOKERTO . 1-2.
- Ariefa, L., & Sundarab, T. A. (2017). Studi atas Pemanfaatan Blockchain bagi Internet of Things (IoT). *JURNAL RESTI*, 71-72.
- Badawi, D. A. (t.thn.). SISTEM VERIFIKASI DOKUMEN HASIL INVESTIGASI FORENSIK DIGITAL BERBASIS TEKNOLOGI BLOCKCHAIN.
- Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. (2018). Decentralized Applications: The Blockchain-Empowered Software System. *IEEE Access*, 3.
- Dzulfikar, F., & Susanto, A. (2020). Implementation of Smart Contracts Ethereum Blockchain in Web-Based Electronic Voting (e-voting). *TRANSFORMTIKA*, 56-60.
- Gupta, R., Jha, B., Shukla, A. K., Raj, A., & Sultana , S. (2020). Secure and Decentralized Smart Elections. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 53-55.
- H, S. D., Palit, H. N., & Handojo, A. (t.thn.). Implementasi Blockchain: Studi Kasus e-Voting.
- Hoti, A., & Chauhan, R. (2020). Development tools for Dapp of Ethereum in Blockchain. *Journal of Xi'an University of Architecture & Technology*, 43.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

- Khan, S. M., Arshad, A., Mushtaq, G., Khaliq, A., & Husein, T. (2020). Implementation of Decentralized Blockchain E-voting. *EAI Endorsed Transactions on Smart Cities*.
- Kurniawan, F., Kusyanti, A., & Nurwarsito, H. (2017). Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 804-805.
- Muid, A., Sholihin, M., & Wardhani, R. (2017). APLIKASI E-VOTING TERHADAP PEMILIHAN PRESIDEN BADAN EKSEKUTIF MAHASISWA UNIVERSITAS ISLAM LAMONGAN. *J-TIIES*, 39-40.
- Noorsanti, R. C., Yulianton, H., & Hadiono, K. (2018). BLOCKCHAIN - TEKNOLOGI MATA UANG KRIPTO (CRYPTO CURRENCY). *Prosiding SENDI_U*, 306-308.
- Nugraha, A. C. (2020). Penerapan Teknologi Blockchain dalam Lingkungan Pendidikan. *Jurnal PRODUKTIF*, 16-17.
- Palopak, Y. (2018). IMPLEMENTASI SISTEM E-VOTING BERBASIS ANDROID PADA SISTEM PEMILIHAN LANGSUNG DI LINGKUNGAN UNIVERSITAS ADVENT INDONESIA MENGGUNAKAN FRAMEWORK LARAVEL. *Jurnal TelKa*, 19-20.
- Prabandari, D. A., Bhawiyuga, A., & Amron, K. (2019). Implementasi Permissioned Blockchain Berbasis Hyperledger Sebagai Penjamin Integritas Data Pada Sistem E-Vote. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 5480-5481.
- Prasetyo, A. F., & Munir, R. (t.thn.). Aplikasi Voting Online dengan Menggunakan Teknologi Blockchain.
- Ridwan, M., Arifin, Z., & Yulianto. (2016). RANCANG BANGUN E-VOTING DENGAN MENGGUNAKAN KEAMANAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) BERBASIS WEB (STUDI KASUS : PEMILIHAN KETUA BEM FMIPA) . *Jurnal Informatika Mulawarman*, 22.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

- a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
- b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

- Sabrina, T., Budiyo, A., & Widjajarto, A. (2019). ANALISA SUMBER DAYA MEMORI UNTUK IMPLEMENTASI IPFS (INTERPLANETARY FILE SYSTEM) PADA SMART CONTRACT ETHEREUM. *e-Proceeding of Engineering*, 7909.
- Suputra, I., & Nasution, S. D. (2019). Analisa Algoritma SHA-256 Untuk Mendeteksi Orisinalitas Citra Digital. *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, 167-169.
- Setia, T. E., & Susanto, A. (2019). Smart Contract Blockchain pada E-Voting. *JURNAL INFORMATIKA UPGRIS*, 188.
- Sidiq, M. F., Basuki, A. I., Firdaus, H., & Baihaqi, M. A. (2020). SENTRALISASI PENGAWASAN INFORMASI JARINGAN MENGGUNAKAN BLOCKCHAIN ETHEREUM. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIK)*, 1190.
- Sugiyatno, & Atika, P. D. (2018). DIGITAL SIGNATURE DENGAN ALGORITMA SHA-1 DAN RSA SEBAGAI AUTENTIKASI. *Jurnal Cendikia*, 75-77.
- Tjandra, V. H., & Setiyawati, N. (2019). PERANCANGAN APLIKASI E-VOTING BERBASIS ANDROID DENGAN TEKNOLOGI FIREBASE (STUDI KASUS : PEMILIHAN KETUA HMP FTI UKSW). *Jurnal SITECH*, 22-23.
- Wandani, K. D., & Sinurat, S. (2018). IMPLEMENTASI SECURE HASH ALGORITMA UNTUK PENGAMANAN PADA FILE VIDEO. *Majalah Ilmiah INTI*, 235.
- Yeni, M., & Kumala, D. (t.thn.). Teknologi Blockchain untuk Transparansi dan Keamanan pada Era Digital.

DAFTAR RIWAYAT HIDUP

DATA PRIBADI		
	Nama	Muhammad Zakie
	Tempat / Tanggal Lahir	Pd. Merbau, 22 September 1998
	Jenis Kelamin	Laki-Laki
	Status Pernikahan	Belum Menikah
	Anak Ke-	1 (Satu)
	Tinggi Badan	170 cm
	Berat Badan	56 kg
	Kebangsaan	Indonesia
ALAMAT		
Alamat	Jl. Pekanbaru-Bangkinang km.36, Dusun Perambahan, Desa Koto Perambahan, Kampa, Kampar, Riau	
Nomor HP	082286250694	
Email	11751100101@students.uin-suska.ac.id	
RIWAYAT PENDIDIKAN		
Tahun 2004-2005	TK Asiyah Kp. Panjang	
Tahun 2005-2011	SDN 015 Koto Perambahan	
Tahun 2011-2014	MTsN Kampar	
Tahun 2014-2017	SMAN 1 Kampar Timur	

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.