BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

E-voting adalah suatu sistem pemilihan dimana data dicatat, disimpan dan diproses dalam bentuk informasi digital. Dengan kata lain, e-voting merupakan pemungutan suara yang proses pelaksanaannya mulai dari pendaftaran pemilih, pelaksanaan pemilihan, perhitungan suara dan pengiriman hasil suara dilaksanakan secara elektronik (digital)[1]. E-voting merupakan aplikasi yang masih terus dikembangkan dan sangat diminati pengguna sebagai salah satu fitur yang praktis untuk melakukan suatu pemilihan berbasiskan perangkat elektronik pada komputer[2].

Sistem e-voting ini bertujuan untuk meningkatkan partisipasi dan meningkatkan keamanan dalam mengatasi masalah dan tantangan yang terkait dengan pemilu konvensional. Walaupun begitu sistem e-voting ini masih memerlukan sistem keamanan yang kuat karena pada sistem digital terdapat banyak celah keamanan yang bisa digunakan untuk merusak suatu sistem[3]. Dengan menggunakan Blockchain maka setiap transaksi yang terjadi akan di enkripsi menggunakan Secure Hash Algorithm 256 (SHA-256) dan secara bersambung sehingga terbentuk seperti rantai atau block dan kemudian dikirimkan ke seluruh jaringan yang terkoneksi dengannya secara peer – to – peer sehingga semua dapat memvalidasi transaksi tersebut dan tidak dibutuhkan server tunggal untuk menyimpan datanya[4].

Selain Blockchain dapat mendukung sistem e-voting, Blockchain (distributed ledger) merupakan database yang terdistribusi yang menyimpan catatan yang terus bertambah Untuk itu perlu dibuat sebuah sistem yang dapat menjamin akurasi hasil

e-voting, integritas data ketika melakukan pengiriman hasil voting dari pemilih ke sistem, dan memvalidasi pemilih yang sesungguhnya dalam penerimaan hasil voting[5]. Blockchain bagian dasar dari sebuah desain arsitektur cryptocurrency Bitcoin yang diciptakan oleh Satoshi Nakamoto pada tahun 2008[6]. Ini merupakan bentuk dari distributed database yang mana berisi dari transaksi-transaksi yang disimpan dalam sebuah block data. Setiap block memiliki hash unik yang dihasilkan dari isi dari block itu sendiri. Setiap block menyimpan hash dari block sebelumnya sehingga membentuk sebuah rantai (chain) yang disimpan di setiap node dalam Peer-to-peer nethwork[7].

Karena efisiensi dan fungsinya, secara luas dianggap memiliki prospek aplikasi yang revolusioner. Sebagai bagian pendukung dari struktur data, fungsi hash penting untuk memastikan ketersediaan dan keamanan Blockchain[8]. Untuk mengevaluasi keamanan teknologi Blockchain, penting untuk menganalisis beberapa kriteria keamanan dari fungsi hash yang digunakan dalam Blockchain[9]. hash sendiri merupakan transformasi larik masukan dari data panjang sembarang menjadi string keluaran dengan panjang tetap. Nilai hash tersebut harus memenuhi persyaratan tertentu yang disebut dengan difficulty agar dapat dianggap block yang sah. Pengecekan nilai hash yang sesuai dengan persyaratan itulah yang dinamakan Proof Of Work [10]. Transformasi semacam itu juga disebut fungsi hash atau fungsi collapsing, dan hasilnya disebut hash, kode hash, jumlah hash, atau block has. Block data terhubung dengan nilai hash dari setiap block sebelumnya, dan buku besar, termasuk semua informasi tentang transaksi, yang disimpan di setiap node dalam jaringan terdistribusi. Buku besar terdistribusi diperbarui dengan membuat konsensus menggunakan protokol konsensus yang ditentukan seperti Proof of Work (PoW) ini membantu seluruh berbagi block data yang sama untuk semua node dari jaringan [11].

Menggunakan beberapa fungsi hash dalam komputasi PoW (Proof-of-work) adalah salah satu pendekatan yang umum diadopsi untuk mencapai resistansi ASIC tersebut. Proof-of-work (PoW) adalah protokol konsensus yang umum digunakan yang membutuhkan banyak komputasi untuk menemukan block baru yang valid. Karena sirkuit terintegrasi khusus aplikasi (ASIC) yang dirancang khusus

untuk komputasi PoW mulai mendominasi operasi konsensus Blockchain, sifat desentralisasi jaringan Blockchain sedang terancam. Banyak mekanisme PoW sedang diusulkan untuk menghentikan penggunaan ASIC dalam operasi consensus[12].

Salah satu teknologi Blockchain penting lainnya yang dapat merevolusi pemungutan suara elektronik adalah Ethereum. ini berfungsi sebagai platform umum untuk pembuatan fungsionalitas khusus dalam bentuk Smart Contract[13]. Sistem yang menggunakan fungsionalitas dan fitur yang ada yang disediakan oleh Ethereum untuk menyediakan kemampuan untuk membuat dan memberi suara pada surat suara. Ini terdiri dari tiga Smart Contract yang dikodekan dalam bahasa Ethereum Solidity, dua skrip yang ditulis dalam JavaScript, dan satu halaman HTML. [14] Untuk menerapkan Smart Contract di Ethereum, transaksi pembuatan khusus dijalankan, yang memperkenalkan kontrak ke Blockchain Selama prosedur ini, kontrak diberikan alamat unik, dalam bentuk pengenal 160-bit, dan kodenya diunggah ke Blockchain. Setelah berhasil dibuat, Smart Contract terdiri dari alamat kontrak, saldo kontrak, kode yang dapat dieksekusi yang telah ditentukan sebelumnya[15]. Selain itu, platform Ethereum dan Solidity terus berkembang dengan sangat cepat dan pengembang dihadapkan pada transformasi berkelanjutan dari fitur platform dan keamanan, saat instruksi baru ditambahkan, dan bug serta risiko keamanan ditemukan. Pengembang harus mempertimbangkan bahwa kode yang ditulis hari ini, mungkin tidak akan dikompilasi dalam beberapa bulan, atau setidaknya harus difaktorkan ulang[16]. Di dasar platform Ethereum berdiri dua jenis entitas, yang disebut akun. Akun dapat dimiliki secara eksternal, yang biasanya dikendalikan oleh aktor manusia melalui akun kontrak. Akun kontrak dikendalikan oleh kode yang akan dijalankan di mesin virtual, yang hanya dapat diaktifkan oleh akun yang dimiliki secara eksternal[17].

Penelitian ini dilakukan untuk menjaga data dari serangan peretas karena project data terbuka yang mengancam harus dijaga dari serangan peretas dan serangan keamanan lainnya karena sifat dari project ini yang cepat dan sementara yang meningkatkan kerentanan.

1.2 IDENTIFIKASI MASALAH

Berdasarkan pada uraian latar belakang, maka dapat dirumusakan masalah-masalah yang ada sebagai berikut :

1. Bagaimana mengintegrasikan keamanan data peserta e-voting menggunakan Blockchain.
2. Bagaimana penerapan e-voting dan Blockchain yang dapat mempermudah penyelenggara dalam melakukan keamanan data menggunakan Blockchain.

1.3 MAKSUD DAN TUJUAN PENELITIAN

Berdasarkan latar belakang masalah, maka maksud dari penelitian tugas akhir ini adalah " Perancangan Aplikasi E-Voting Dengan Sistem Smart Contract Berbasis Teknologi Blockchain". Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Merancang sistem keamanan Blockchain untuk membantu penyelenggaran dalam keamanan data peserta e-voting.
2. Meningkatkan tingkat kepercayaan antara peserta dan penyelenggara karena keamanan penyimpanan data lebih terjaga.
3. Mengurangi terjadinya manipulasi data baik itu data hasil pemilihan atau yang bersifat rahasia lain nya.
4. Menerapkan sistem smart contract pada aplikasi yang akan di bangun untuk menunjang kemudahan dalam menjaga keamanan data pada sistem e-voting berbasis teknologi blockchain.

1.4 BATASAN MASALAH

Adapun pembatasan masalah dari penelitian ini adalah sebagai berikut :

1. Data yang digunakan untuk menguji sistem adalah data dari anggota Himpunan Teknik Inforamtika tahun 2019/2020
2. Pengujian keamanan data menggunakan aplikasi berbasis website.

3. Smart contract yang dibangun menggunakan bahasa pemrograman Solidity dalam menerapkan aplikasi yang terdesentralisasi.

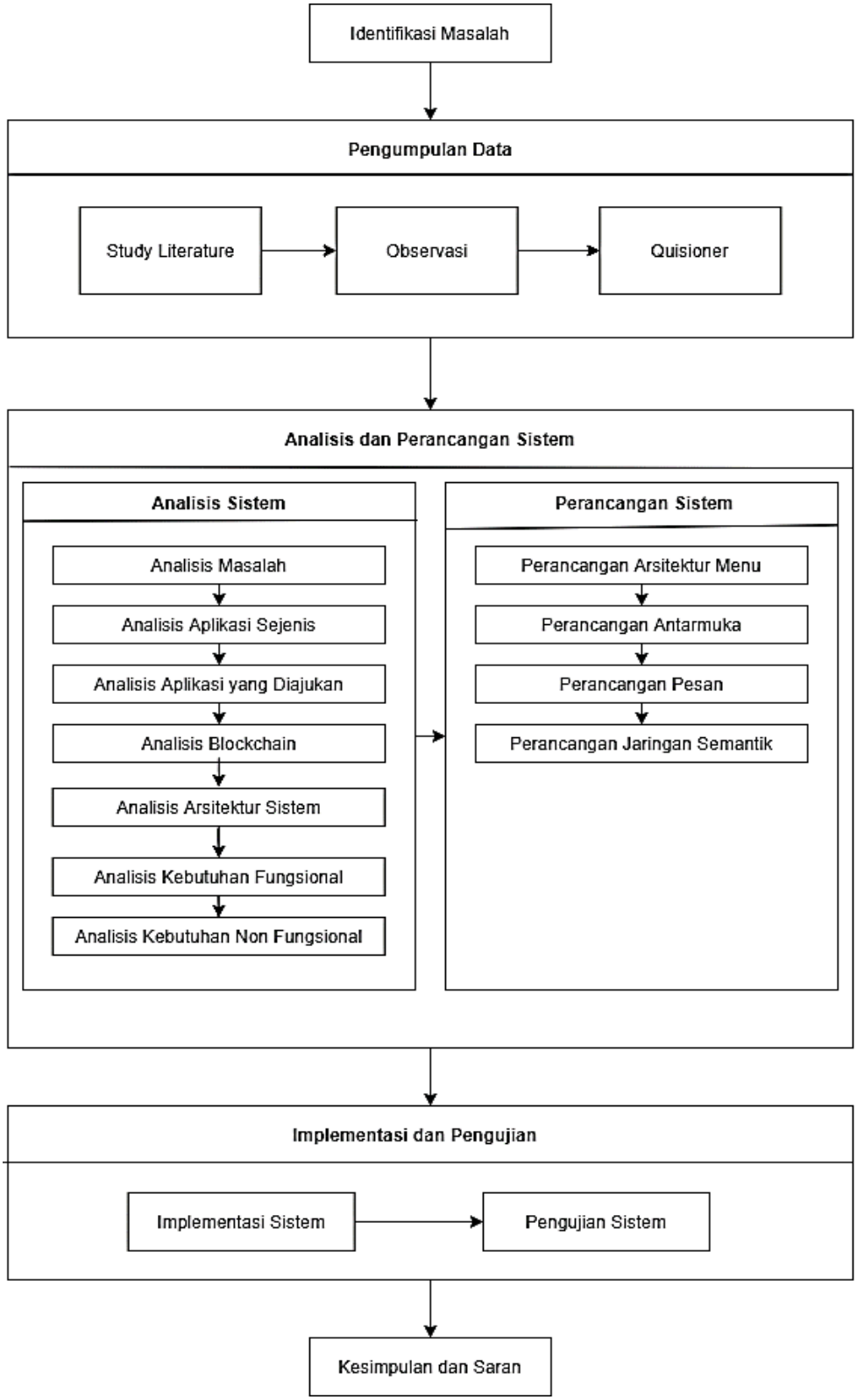
4. Interplanetary File System (IPFS) untuk sistem penyimpanan file dokumen.

5. Dompet digital atau Wallet Ethereum menggunakan Metamask Chrome Extension.

6. Pemodelan sistem menggunakan diagram UML.

1.5 METODOLOGI PENELITIAN

Metodologi penelitian merupakan tahapan - tahapan yang telah ditentukan dalam melakukan sebuah penelitian yang berguna sebagai pedoman dalam melakukan proses penelitian agar penelitian yang dilakukan dapat berjalan dengan baik dan sistematis. Berikut adalah alur dari metodologi penelitian yang digunakan dapat dilihat pada Gambar 1.1.



Gambar 1. 1 Alur Penelitian

Berikut adalah penjelasan setiap alur penelitian dari gambar 1.1 :

1. Identifikasi Masalah

Tahap ini adalah tahap awal penelitian dengan mengidentifikasi serta merumuskan masalah yang terjadi seputar topik penelitian. Pada tahap ini akan dilakukan identifikasi masalah dengan cara menganalisis dan mengevaluasi permasalahan yang terjadi.

2. Pengumpulan Data

Tahap ini adalah tahap dimana rumusan masalah telah didapat serta solusi permasalahan lalu memulai komunikasi dengan pihak yang bersangkutan.

3. Analisis dan Perancangan Sistem

Pada tahap ini akan melakukan analisis dan perancangan sistem dari permasalahan yang telah dirumuskan dan data yang telah diperoleh secara cepat. Selanjutnya akan mengevaluasi permasalahan-permasalahan tersebut dan menganalisis kebutuhan-kebutuhan terkait aplikasi dan perancangan sistem agar tercapainya suatu tujuan penelitian. Pada tahapan ini terbagi menjadi dua yaitu analisis sistem dan perancangan sistem. Analisis sistem terdiri dari analisis masalah, analisis aplikasi sejenis, analisis aplikasi yang diajukan, analisis Blockchain, analisis arsitektur sistem, analisis kebutuhan non-fungsional, dan analisis kebutuhan fungsional. Sedangkan untuk perancangan sistem terdiri dari perancangan arsitektur menu, perancangan arsitektur kontrak, perancangan antarmuka, perancangan pesan, dan perancangan jaringan semantic.

4. Implementasi dan Pengujian

Pada tahap ini mulai membangun sistem dengan penulisan kode sebagai tahap implementasi sistem dan melakukan pengujian sebagai tahap penyerahan untuk mendapatkan umpan balik. Hasil dari perencanaan dan perancangan sistem menjadi dasar dalam melakukan pembangunan Aplikasi. Aplikasi ini akan menghasilkan sebuah sistem yang sebelumnya telah melalui tahap perencanaan dan perancangan. Selanjutnya hasil tersebut akan diuji pada tahap pengujian sistem menggunakan metode black box. Selain itu

pengujian ini juga dimaksudkan untuk bahan evaluasi apakah penelitian yang dilakukan berhasil mencapai tujuan penelitian atau tidak.

5. Kesimpulan dan Saran

Pada tahap ini akan melakukan penarikan kesimpulan atas sistem yang telah dibangun berdasarkan tujuan penelitian. Penelitian akan dikatakan berhasil apabila kesimpulan memenuhi tujuan penelitian. Penarikan kesimpulan ini berdasar pada hasil penelitian yang dilakukan yang merujuk pada tujuan penelitian. Selain penarikan kesimpulan, pada tahap ini juga akan menjabarkan saran untuk pengembangan penelitian dimasa yang akan datang.

1.5.1 Metodologi Pengumpulan Data

Adapun pengumpulan data yang digunakan pada penelitian ini adalah sebagai berikut :

a. Studi Literatur

Studi literatur merupakan pengumpulan data yang meneliti berbagai macam dokumen yang berguna untuk bahan analisis dan tidak ditujukan langsung kepada subjek penelitian. Data tersebut merupakan daftar pustaka yang berupa artikel, jurnal, buku, dan laporan akhir yang ada kaitannya dengan judul penelitian.

b. Observasi

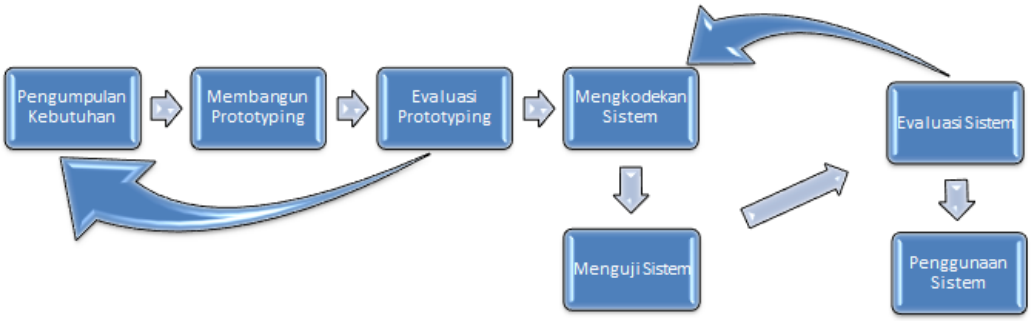
Observasi adalah teknik pengumpulan data dengan melihat situasi peneliti dalam melihat situasi penelitian. Beberapa informasi yang diperoleh dari hasil observasi adalah ruang (tempat), pelaku, kegiatan atau peristiwa, dan waktu.

c. Kuisioner

Kuesioner merupakan metode pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawab.

1.5.2 Metodologi Pembangunan Perangkat Lunak

Metode pembangunan perangkat lunak yang digunakan dalam penelitian ini adalah metode Prototyping karena dalam pembangunannya keterlibatan pengguna sangat tinggi sehingga sistem dapat memenuhi kebutuhan pengguna.



Gambar 1. 2 Metode Pembangunan Perangkat Lunak

Berikut adalah tahap – tahap yang dilakukan dalam melakukan metode Prototyping [15] :

1. **Pengumpulan Kebutuhan** Pelanggan dan pengembang bersama-sama mendefinisikan format seluruh perangkat lunak, mengidentifikasikan semua kebutuhan, dan garis besar sistem yang akan dibuat.
2. **Membangun Prototyping** Membangun prototyping dengan membuat perancangan sementara yang berfokus pada penyajian kepada pelanggan (misalnya dengan membuat input dan format output).
3. **Evaluasi Prototyping** Evaluasi ini dilakukan oleh pelanggan apakah prototyping yang sudah dibangun sudah sesuai dengan keinginan pelanggan. Jika sudah sesuai maka langkah 4 akan diambil. Jika tidak prototyping direvisi dengan mengulang langkah 1, 2 , dan 3.

4. **Mengkodekan Sistem** Dalam tahap ini prototyping yang sudah disepakati diterjemahkan ke dalam bahasa pemrograman yang sesuai.
5. **Menguji Sistem** Setelah sistem sudah menjadi suatu perangkat lunak yang siap pakai, harus dites dahulu sebelum digunakan. Pengujian ini dilakukan dengan White Box, Black Box, Basis Path, pengujian arsitektur dan lain-lain.
6. **Evaluasi Sistem** Pelanggan mengevaluasi apakah sistem yang sudah jadi sudah sesuai dengan yang diharapkan. Jika ya, langkah 7 dilakukan; jika tidak, ulangi langkah 4 dan 5.
7. **Menggunakan Sistem** Perangkat lunak yang telah diuji dan diterima pelanggan siap untuk digunakan.

1.6 HIPOTESIS PENELITIAN

Sistematika penulisan tugas akhir ini disusun untuk memenuhi gambaran umum tentang penelitian yang dilakukan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi uraian latar belakang masalah, identifikasi masalah, maksud dan tujuan, batasan masalah, metodologi penelitian yang digunakan serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan membahas berbagai konsep-konsep dasar dan teori-teori pendukung yang berhubungan dengan pembangunan sistem. Seperti pembahasan mengenai E-voting, Blockchain, Ethereum Virtual Machine, Ethereum, Smart Contract, Solidity dan tool yang digunakan.

BAB III ANALISIS DAN PERANCANGAN KEBUTUHAN

Pada bab ini berisi pemaparan analisis masalah, analisis aplikasi sejenis, analisis arsitektur sistem, analisis kebutuhan non-fungsional dan fungsional. Hasil

dari analisis tersebut digunakan untuk melakukan perancangan perangkat lunak yang terdiri dari perancangan arsitektur menu, perancangan arsitektur kontrak, dan sebagainya.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Pada bab ini berisi hasil implementasi analisis dari BAB 3 dan perancangan aplikasi yang dilakukan, serta hasil pengujian sistem untuk mengetahui apakah sistem yang dibangun sudah memenuhi kebutuhan.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan yang diperoleh dari hasil pengujian sistem, serta saran untuk pengembangan sistem terdesentralisasi yang telah dirancang.