**SISTEM VOTING ELEKTRONIK BERBASIS ETHEREUM SMART CONTRACT**

**TUGAS AKHIR**

Diajukan guna memenuhi sebagian persyaratan dalam rangka menyelesaikan Pendidikan Sarjana Strata Satu (S1) Program Studi Teknologi Informasi



**I DEWA GEDE DIRGA YASA**

**NIM: 1705551062**

**PROGRAM STUDI TEKNOLOGI INFORMASI**

**FAKULTAS TEKNIK**

**UNIVERSITAS UDAYANA**

**2021**

**SISTEM VOTING ELEKTRONIK BERBASIS ETHEREUM SMART CONTRACT**

**TUGAS AKHIR**

Diajukan guna memenuhi sebagian persyaratan dalam rangka menyelesaikan Pendidikan Sarjana Strata Satu (S1) Program Studi Teknologi Informasi



**I DEWA GEDE DIRGA YASA**

**NIM: 1705551062**

**PROGRAM STUDI TEKNOLOGI INFORMASI**

**FAKULTAS TEKNIK**

**UNIVERSITAS UDAYANA**

**2021**

# KATA PENGANTAR

Puji dan syukur saya panjatkan kehadapan Tuhan Yang Maha Esa sehingga penulis dapat menyelesaikan tugas akhir dengan judul **“Sistem Voting Elektronik Berbasis Ethereum Smart Contract”**. Dalam penyusunan Tugas Akhir ini, penulis mendapatkan masukan dan bimbingan dari berbagai pihak. Sehubungan dengan hal tersebut pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Prof. Ir. Ngakan Putu Gede Suardana, MT, Ph.D selaku Dekan Fakultas Teknik Universitas Udayana.
2. Dr. Ir. I Made Oka Widyantara, ST., MT., IPM, ASEAN Eng. selaku Koordinator Program Studi Teknologi Informasi Fakultas Teknik Universitas Udayana.
3. Bapak I Putu Arya Dharmadi, S.T.,M.T. selaku dosen pembimbing I yang telah banyak meluangkan waktu memberikan dorongan, bimbingan, tuntunan dan kesabaran selama penyusunan Tugas Akhir ini.
4. Bapak A. A. Kt. Agung Cahyawan Wiranatha, S.T.,M.T. selaku dosen pembimbing II yang juga telah banyak meluangkan waktu memberikan dorongan, bimbingan, tuntunan dan kesabaran selama penyusunan Tugas Akhir ini.
5. Segenap dosen pengajar yang turut memberikan ilmu dan pengetahuan selama penulis menempuh perkuliahan di Program Studi Teknologi Informasi Fakultas Teknik Universitas Udayana.
6. Bapak dan Ibu pegawai di Program Studi Teknologi Informasi Fakultas Teknik Universitas Udayana yang telah membantu selama proses perkuliahan dan administrasi.
7. Orang tua serta anggota keluarga yang telah banyak memberikan motivasi dan dukungan baik jasmani maupun rohani selama penulis menyusun Tugas Akhir ini.
8. Teman-teman seperjuangan dan segenap civitas di Program Studi Teknologi Informasi Universitas Udayana yang telah memberikan sumbangan ide dan dukungan dalam penyusunan Tugas Akhir ini.
9. Berbagai pihak yang belum dapat disebutkan satu-persatu yang juga berperan penting dalam membatu, memberikan sumbangan ide, pemikiran dan dukungan dalam penyusunan Tugas Akhir ini

Penulis menyadari bahwa laporan ini jauh dari sempurna baik dalam materi maupun penulisannya. Berkaitan dengan hal tersebut, maka kritik dan saran yang bersifat membangun dari semua pihak sangat diharapkan. Akhir kata, semoga laporan ini dapat memberikan manfaat bagi semua pihak sesuai dengan yang diharapkan.

Denpasar, Mei 2021

I Dewa Gede Dirga Yasa

# ABSTRAK

# ABSTRACT

# DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR KODE PROGRAM

# DAFTAR TABEL

# BAB I PENDAHULUAN

Bab I berisi bahasan mengenai pendahuluan dari penelitian ini. Pendahuluan dijabarkan menjadi beberapa bagian, diantaranya latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, dan sistematika penulisan.

## Latar Belakang

Pengambilan keputusan bersama memiliki beberapa cara dalam pelaksanaannya, diantaranya musyawarah mufakat, voting dan aklamasi. Masing-masing metode pengambilan keputusan memiliki kelebihan dan kekurangan. Metode pengambilan keputusan yang paling sering digunakan adalah voting karena keputusan dapat dihasilkan dalam jangka waktu yang relatif cepat. Kegiatan yang paling sering menggunakan metode voting adalah pemilihan kepala daerah karena voting sesuai dengan prinsip demokrasi yang memberikan kesempatan setiap kalangan untuk memberikan hak suara. Seiring dengan berkembangnya teknologi, kecepatan dalam mengakses informasi adalah prioritas sehingga cara voting konvensional yang menggunakan kertas dan paku bukan menjadi pilihan yang optimal.

Berdasarkan permasalahan di atas, negara-negara di dunia mulai mengembangkan voting elektronik atau yang biasa disebut dengan *e-voting*. *E-voting* memiliki beberapa model yang digunakan yaitu *internet poll site voting*, *kiosk voting* dan *internet voting*. *Internet poll site voting* merupakan model *e-voting* yang menggunakan komputer di lokasi pemilihan dan menggunakan internet untuk mengirim data dari lokasi pemilihan ke otoritas penyelenggara pemilihan. Sehingga pemilih masih harus datang ke lokasi pemilihan untuk melakukan voting. *Kiosk voting* adalah model *e-voting* yang pemilihnya bisa menggunakan komputer di lokasi yang sudah menjalankan kerja sama dengan otoritas penyelenggara pemilihan misalnya komputer di perpustakaan daerah, sekolah dan *mall*. Sedangkan *internet voting* adalah model *e-voting* yang sepenuhnya menggunakan internet sehingga pemilih dapat melakukan voting dari perangkat masing-masing (Muhammad Habibi, 2018.). Model *e-voting internet poll site voting* dan *kiosk voting* dirasa kurang optimal karena walaupun sudah menggunakan teknologi internet, pemilih masih belum bisa menggunakan perangkat yang dimiliki sehingga tetap harus datang ke tempat pemilihan untuk melakukan voting. Saat ini, era dimana kecepatan dan kemudahan akses informasi menjadi prioritas, internet voting menjadi model *e-voting* yang paling optimal untuk dikembangkan.

Beberapa negara yang sudah mengembangkan *e-voting* model internet voting diantaranya Australia, Kanada, Jepang, Jerman dan Inggris (Muhammad Habibi, 2018). *E-voting* berjalan dengan lancar di Australia, Kanada dan Jepang namun gagal di Jerman dan Inggris. *E-voting* juga memiliki beberapa masalah yang membuat *e-voting* mendapatkan penolakan oleh masyarakat yaitu masalah kerahasiaan dan kepercayaan terhadap data. Salah satu teknologi yang dapat mengatasi masalah tersebut adalah *blockchain*.

*Blockchain* merupakan teknologi terdistribusi yang memungkinkan pengguna atau komunitas pengguna untuk menambahkan data yang akan tercatat dalam sebuah jaringan, namun data yang telah ditambahkan tidak dapat diubah kembali. Hal tersebut tentunya menyebabkan *blockchain* dianggap menjadi teknologi yang tangguh dan tidak ada celah untuk melakukan modifikasi ataupun manipulasi data.

## Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka diperoleh beberapa rumusan masalah sebagai berikut.

1. Bagaimana proses kerja *Ethereum Smart Contract* pada Sistem Voting Elektronik*.*
2. Bagaimana perancangan dan proses pembangunan Sistem Voting Elektronik berbasis *Ethereum smart contract*.
3. Bagaimana hasil penelitian dan kinerja Sistem Voting Elektronik berbasis *Ethereum smart contract*.

## Tujuan

Berdasarkan rumusan masalah yang telah dipaparkan sebelumnya, maka diperoleh tujuan sebagai berikut.

1. Memahami proses kerja Sistem Voting Elektronik berbasis *Ethereum smart contract*.
2. Mengetahui perancangan dan proses pembangunan Sistem Voting Elektronik berbasis *Ethereum smart contract*.
3. Mengetahui hasil penelitian dan kinerja Sistem Voting Elektronik berbasis *Ethereum smart contract*.

## Manfaat Penelitian

Penelitian ini dalam pelaksanaannya memiliki beberapa manfaat yang dijabarkan sebagai berikut.

1. Menghilangkan *trust issue* dalam pelaksanaan voting.
2. Meningkatkan keamanan data hasil voting.
3. Menghemat waktu dalam proses pengambilan data voting.
4. Meminimalisir biaya yang perlu dikeluarkan dalam proses pengambilan data voting.
5. Mempermudah proses pengambilan data voting karena dapat dilakukan dari mana saja melalui perangkat pengguna yang terkoneksi internet.

## Batasan Masalah

Penelitian ini dalam pelaksanaannya memiliki beberapa batasan yang bertujuan agar penggunaan aplikasi tidak terlalu luas. Batasan masalah yang dijabarkan adalah sebagai berikut.

1. Penelitian yang dilakukan hanya berfokus pada Sistem Voting Elektronik.
2. *Platform blockchain* yang digunakan adalah *Ethereum.*

## Sistematika Penulisan

Sistematika penulisan merupakan bagian yang menjelaskan gambaran laporan dari semua dasar teori dan metode yang digunakan serta hasil yang diperoleh selama pengerjaan tugas akhir. Laporan tugas akhir ini dibagi menjadi lima bab sebagai berikut.

BAB I : **Pendahuluan**

Bagian ini membahas mengenai latar belakang, perumusan masalah, tujuan, manfaat, batasan masalah, serta sistematika penulisan laporan tugas akhir Sistem Voting Elektronik Berbasis *Ethereum Smart Contract*.

BAB II : **Tinjauan Pustaka**

Bagian ini menjelaskan tentang dasar teori, pengetahuan, dan referensi yang digunakan untuk memperkuat projek Tugas Akhir Sistem Voting Elektronik Berbasis *Ethereum Smart Contract*.

BAB III : **Metodologi dan Perancangan Sistem**

Bagian ini memuat metode yang digunakan dalam penelitian tugas akhir Sistem Voting Elektronik Berbasis *Ethereum Smart Contract* beserta dengan proses pembuatan laporan yang meliputi tempat dan waktu penelitian, sumber data dan metode pengumpulan, instrumen perancangan, algoritma pemrograman, hingga perancangan sistem dimulai dari rancangan prosedural hingga antarmuka (*interface*) sistem.

BAB IV : **Pengujian dan Analisa Hasil**

Bagian ini memuat rancangan yang telah dibuat, implentasi dari perangkat yang digunakan serta pengujian sistem dari Sistem Voting Elektronik Berbasis *Ethereum Smart Contract*.

BAB V : **Penutup**

Bagian ini memuat kesimpulan yang mengacu pada rumusan masalah dan tujuan penelitian beserta saran yang diberikan peneliti untuk kepentingan pengembangan aplikasi selanjutnya.

# BAB II TINJAUAN PUSTAKA

Bab II berisi bahasan mengenai teori atau materi pendukung yang digunakan sebagai acuan atau dasar teori dalam Sistem Voting Elektronik Berbasis *Ethereum Smart Contract*.

## *State of the Art*

Perancangan untuk pengembangan Sistem Voting Elektronik memiliki persamaan dan atau keterikatan dari beberapa penelitian yang dilakukan beberapa diantaranya adalah sebagai berikut.

Penelitian pertama yang digunakan sebagai acuan dalam penelitian ini adalah penelitian mengenai pengembangan sistem E-Voting berbasis *web* menggunakan keamanan algoritma Rivest Shamir Adleman (RSA). Aplikasi ini dibangun menggunakan bahasa pemrograman PHP dan *database* MySQLi sebagai *database server*. Fokus dari sistem voting elektronik ini adalah melakukan enkripsi hak suara pemilih pada sistem menggunakan *public key* dan *private key* untuk proses verifikasi sehingga tidak ada manipulasi data hak suara pemilih. Hasil yang diperoleh adalah sistem dapat melakukan validasi pemilih dan melakukan verifikasi hak suara apakah telah terjadi manipulasi data selama pengiriman atau tidak (Ridwan, et al., 2016). Penelitian selanjutnya adalah penelitian mengenai sistem *e-voting* berbasis SMS *gateway* yang dirancang menggunakan *software* Gammu dan menggunakan bahasa pemrograman PHP dan *database* MySQL. Uji coba pemungutan suara dilakukan dengan mengirim pemberitahuan melalui SMS kepada pemilih sesuai dengan data yang telah disimpan dan pemilihan dilakukan dengan cara mengirim SMS balasan sesuai dengan format yang telah ditentukan (Adhi & Harjono, 2014).

Perancangan sistem *voting* elektronik juga diterapkan dalam penelitian menggunakan *smart contract blockchain*. Sistem dirancang menggunakan bahasa pemrogaman *solidity* dan *smart contract* menghasilkan kode unik pada setiap pemilihan baru. Pengujian menghasilkan bahwa manipulasi hasil pemungutan suara tidak dapat dilakukan karena setiap pemilih hanya dapat memiliki satu akun dan satu *address blockchain* (Setia & Susanto, 2019). Perancangan sistem *e-voting* juga diterapkan menggunakan metode enkripsi *blockchain.* Enkripsi *blockchain* merupakan salah satu cara pengamanan data yang tidak memungkinkan untuk dilakukan penyusupan data ke dalamnya serta menjaga kerahasiaan pada data pemilih karena dilakukan proses enkripsi pada data pemilih dan apa yang dipilih, akan tetap dapat diperoleh informasi pemilik suara terbanyak (Ardilla, 2018). Penelitian lain terhadap sistem *e-voting* menggunakan teknologi *blockchain* adalah penelitian oleh Kurnia Hu, dkk menggunakan *multichain tools.* Penelitian ini menghasilkan sistem voting elektronik yang dapat menyimpan data yang transparan dan dapat diakses oleh publik, menjaga identitas pemilih, menyimpan data suara yang tidak dapat diubah, digandakan, atau dihapus. Berdasarkan hasil kuesioner diperoleh persentase sebesar 55,6 % pengguna menilai baik dan 44,4 % pengguna menilai baik sekali mengenai keseluruhan aplikasi (Kurnia Hu, et al., 2019). Aplikasi *e-voting* selanjutnya adalah SEVA: Secure E-Voting Application. Sistem dirancang bertujuan untuk memungkinan bagi para pemilih dapat melakukan pemilihan melalui *web* tanpa terbatas oleh lokasi. Aplikasi dikembangkan dengan Azure Service Fabric menggunakan arsitektur Microservice. Aplikasi ini diterapkan pada cluster Five-Node menggunakan Server Fabric Local Cluster (Johari, et al., 2020).

Penelitian selanjutnya adalah penerapan teknologi *blockchain* dalam layanan *E-commerce* pada OJS (*Open Journal System*)*.* Penggunaan teknologi *blockchain* dalam penelitian ini bertujuan untuk mengefisiensi manajemen identitas, membangun sistem pelacakan dan mengidentifikasi keaslian produk, dapat menyinkronkan data yang tersimpan dalam *blockchain* ke semua jaringan pengguna, dapat menjadikan sistem pembayaran yang lebih mudah, efisien dan terdokumentasikan dengan baik. Serta kemudahan bagi mahasiswa, dosen dan pihak lain dalam melakukan proses transaksi (Rahardja, et al., 2020)*.*

## Blockchain

*Blockchain* adalah teknologi pencatatan transaksi yang menghilangkan pihak ketiga atau *central authority* dalam melakukan pertukaran data atau transaksi. *Blockchain* juga dapat dikatakan sebagai buku besar digital dimana setiap transaksi yang terjadi di jaringan *blockchain* akan dicatat dan diamankan di dalam *peer* atau *node* yang terlibat di jaringan *blockchain*. Secara umum cara kerja *blockchain* adalah transaksi yang terjadi di jaringan *blockchai*n akan dicatat dalam blok. Blok akan menghasilkan sebuah *hash*. *Hash* blok pada transaksi sebelumnya akan dicatat di blok saat ini. Begitu pula *hash* blok saat ini akan dicatat di blok selanjutnya sehingga akan menghasilkan struktur seperti rantai (Pierro, 2017).

|  |
| --- |
|  |

Gambar 2. 1 Arsitektur *Blockchain*

Jika ada pihak yang ingin melakukan kecurangan dengan cara mengubah data transaksi dalam suatu blok, maka pihak tersebut harus melakukan *hashing* ulang dari blok yang diubah hingga blok yang terjadi saat ini. Tidak hanya itu, karena blok disimpan secara terdistribusi, maka pihak tersebut juga harus mengubah data blok di setiap *node* yang terlibat dalam jaringan. Hal inilah yang menjadi kekuatan *blockchain* sehingga dapat menghilangkan *central authority* dalam melakukan transaksi.

## Ethereum

Ethereum adalah sebuah blockchain yang didirikan pada tahun 2015 yang digagas oleh Vitalik Buterin. Salah satu tujuan pengembangan Ethereum adalah untuk memberikan kemampuan eksekusi program komputer pada blockchain. Aplikasi terdesentralisasi yang memanfaatkan kemampuan eksekusi program komputer ini sering disebut dengan *dapps.*

### Ethereum Accounts dan Transaction

Accounts adalah entitas yang terdapat dalam Ethereum yang dapat membuat Transaction dimana setiap account memiliki address yang panjangnya 20-bytes. Sebuah Etherum account memiliki empat field yaitu nonce, ether balance, contract code dan storage. Nonce adalah counter yang digunakan untuk memastikan bahwa setiap transaksi yang dibuat oleh sebuah account hanya diproses sekali. Ether atau (ETH) adalah mata uang digital yang digunakan untuk membayar biaya transaksi. Secara umum ada dua jenis account yang terdapat di Ethereum. Yang pertama adalah Externally Owned Account (EOA) yang dikontrol menggunakan private key dan yang kedua adalah contract account yang dikontrol oleh contract code-nya. Contract account bisa dikatakan sebagai autonomous agents yang hidup didalam Ethereum execution environment yang selalu menjalankan perintah spesifik dari kode ketika menerima transaksi.

Istilah transaksi yang dimaksud dalam Ethereum adalah data yang telah ditandatangani secara digital oleh sebuah EOA. Sebuah transaksi berisi address penerima, signature untuk identifikasi pengirim, jumlah ether yang akan dikirim, data field, gas dan gas price. Gas adalah nilai yang merepresentasikan seberapa besar transaksi tersebut boleh menggunakan resource komputasi.

### Ethereum Code Execution

Kode dalam kontrak Ethereum ditulis dalam sebuah bahasa bytecode low-level berbasis stack yang disebut sebagai Ethereum virtual machine code atau EVM Code. Kode terdiri dari beberapa kumpulan byte dimana setiap kumpulan byte merepresentasikan sebuah operasi. Secara umum, code execution ada sebuah perulangan tak hingga yang melakukan increment penambahan satu yang dimulai dari nol hingga program mencapai error atau terdeteksi intruksi return. Setiap operasi memiliki akses ke tiga jenis penyimpanan data yaitu stack, memory dan storage. Stack adalah sebuah contrainer last-in-first-out dimana nilainya bisa di pushed atau pop. Memory adalah expandable byte array yang akan hilang ketika komputasi selesai dilakukan. Storage adalah penyimpanan persistent yang menyimpan data menggunakan model key/value.

### Openethereum

Jaringan suatu blockchain tercipta dari jaringan komunikasi peer-to-peer dari beberapa nodes. Nodes adalah suatu program komputer yang berjalan berdasarkan spesifikasi suatu blockchain. Hal yang sama juga berlaku pada jaringan Ethereum. Nodes pada jaringan Ethereum adalah program yang berjalan berdasarkan spesifikasi Ethereum. Ada beberapa Ethereum client yang ada saat ini yaitu geth, openethereum, nethermind dan hyperledger besu. Ethereum client tersebut menggunakan bahasa pemrograman yang berbeda namun tetap bisa saling berkomunikasi karena mengimplementasikan spesifikasi yang sama.

Openethereum adalah sebuah Ethereum client yang dibuat menggunakan bahasa pemrograman Rust. Keunggulan yang dimiliki oleh Openethereum adalah program yang ringan, kecepatan sinkronisasi dan dokumentasi yang jelas tentang bagaimana cara mengoptimalisasikan Openethereum untuk skenario penggunaan yang berbeda.

### Smart Contract

Smart Contract adalah kumpulan dari kode dan data yang teridentifikasi menggunakan sebuah address pada blockchain Ethereum. Smart Contract merupakan salah satu jenis Ethereum account sehingga sebuah Smart Contract bisa menyimpan ETH dan mengirim transaksi di jaringan blockchain. Akan tetapi Smart Contract tidak dikendalikan oleh seorang pengguna atau EOA. Sebuah Smart Contract akan di-deploy ke jaringan blockchain dan bekerja sesuai kode yang dimilikinya. Seorang pengguna bisa beriteraksi dengan sebuah Smart Contract dengan cara membuat sebuah transaksi dengan menggunakan address Smart Contract sebagai recipient.

Kode Smart Contract dapat dibuat dengan bahasa pemrograman yang lebih mudah dipahami yaitu Solidity. Solidity adalah bahasa pemrograman yang diusulkan oleh Gavin Wood pada tahun 2014. Hingga saat ini Solidity menjadi bahasa pemrograman terpopuler untuk membuat Smart Contract karena Solidity didesain menyerupai ECMAScript sehingga lebih familiar di kalangan developer.

### Konsensus

Secara umum pengertian konsensus adalah sebuah kesepakatan bersama yang telah dicapai oleh suatu kelompok terhadap suatu masalah. Konsensus dalam blockchain sangat penting karena data yang terdesentralisasi sehingga sangat memungkinkan terjadinya perbedaan daya yang tercatat. Dengan adanya algoritma konsensus ini maka jaringan tidka akan kebingungan ketika terjadi perbedaan pencatatan data dan menentukan data mana yang akan digunakan. Sebagian besar ekosistem blockchain saat ini menggunakan algoritma Proof of Work sebagai konsensus di jaringa blockchain.

Cara kerja algoritma konsensus Proof of Work adalah setiap node yang tergabung dalam sebuah jaringan blockchain akan berlomba untuk memproses transaksi yang terjadi dalam kurun waktu tertentu dan node tercepat yang bisa menyelesaikan pembuatan blok baru akan menyebarkan block tersebut ke jaringan. Account yang terhubung dengan node tersebut akan mendapatkan insentif sesuai dengan mata uang jaringan blockchain. Sedangkan algoritma konsensus Proof of Authority, dalam jaringan sudah di atur account mana saja yang boleh melakukan pembuatan blok. Karena account yang melakukan pembuatan blok sudah ditentukan sehingga tidak akan terjadi persaingan dalam hal pembuatan blok sehingga tingkat difficulty dari pembuatan blok bisa diturunkan. Dengan tingkat difficulty yang rendah maka jaringan dapat berjalan dengan komputer dengan daya komputasi rendah sehingga bisa menghemat biaya infrastruktur.

### Gas, Gas Fee dan Gas Limit

*Gas* adalah sebuah kalkulasi untuk menentukan seberapa besar biaya yang dibutuhkan untuk melakukan tindakan pada jaringan blockchain. Semua aktivitas yang dilakukan pada jaringan Ethereum seperti pengiriman ETH hingga pemanggilan metode Smart Contract membutuhkan *gas*. *Gas* yang dibutuhkan harus dibayar menggunakan ETH. Besarnya biaya *gas* yang harus dibayarkan ini biasanya disebut dengan *gas fee. Gas limit* adalah batas maksimal *gas* yang boleh digunakan untuk melakukan sebuah transaksi. *Gas limit* sangat penting karena jika tidak ada *gas limit* maka jika terjadi suatu kesalahan misalnya kesalahan *smart contract* yang menyebabkan pemanggilan berulang akan terus menggunakan ETH yang terdapat pada account eksekutor untuk membayar *gas* hingga ETH pada account tersebut habis.

## VSCode

Visual Studio Code adalah sebuah teks editor ringan dan handal yang dibuat oleh Microsoft untuk sistem operasi *multiplatform*, artinya tersedia juga untuk versi Linux, Mac, dan Windows. Teks editor ini secara langsung mendukung bahasa pemrograman JavaScript, Typescript, dan Node.js, serta bahasa pemrograman lainnya dengan bantuan *plugin* yang dapat dipasang melalui *marketplace* Visual Studio Code (seperti C++, C#, Python, Go, Java, dst).

Fitur-fitur yang disediakan oleh Visual Studio Code, diantaranya *Intellisense, Git Integration, Debugging,* dan fitur ekstensi yang menambah kemampuan teks editor. *Editor* ini dirancang untuk pengembang yang bekerja dengan teknologi *open source* *cloud* serta menggunakan NET untuk memberikan dukungan untuk ASP. Antarmukanya tergolong mudah untuk digunakan karena didasarkan pada gaya *explorer* umum, dengan *panel* di sebelah kiri yang menunjukkan semua *file* dan *folder* serta *panel editor* di sebelah kanan, yang menunjukkan isi dari *file* yang telah dibuka.

|  |
| --- |
| https://code.visualstudio.com/opengraphimg/opengraph-home.png |

Gambar 2. 2 Visual Studio Code

Microsoft telah menyediakan dokumentasi yang lengkap untuk membantu dan memudahkan penggunaan bagi para *developer*. Visual Studio Code ditargetkan pada pengembang scripting *server-side* dan dapat digunakan oleh siapa saja untuk membangun aplikasi berbasis *web* (Code, 2021)*.*

## NodeJS

Node.js merupakan salah satu *platform* pengembang yang dapat digunakan untuk membuat aplikasi berbasis *Cloud*. Node.js dikembangkan dari *engine* JavaScript yang dibuat oleh Google untuk *browser* Chrome ditambah dengan *libuv* serta beberapa pustaka lainnya. Node.js menggunakan JavaScript sebagai bahasa pemrograman dan *event-driven, non-blocking I/O (asynchronous)* model yang membuatnya ringan dan efisien. Node.js memiliki fitur built-in HTTP *server library* yang menjadikannya mampu menjadi sebuah *web server* tanpa bantuan *software* lainnya seperti Apache dan Nginx.

|  |
| --- |
| https://miro.medium.com/max/724/1*ODU5V_oAmYmzvZ1wIw3rDw.png |

Gambar 2. 3 Node.js

Sumber : https://ichi.pro/id

Node.js adalah sebuah *runtime environment* dan *script library*. Sebuah *runtime environment* adalah sebuah *software* yang berfungsi untuk mengeksekusi, menjalankan dan mengimplementasikan fungsi-fungsi serta cara kerja inti dari suatu bahasa pemrograman. Sedangkan *script library* adalah kumpulan, kompilasi atau bank data berisi skrip/kode-kode pemrograman. Node.js dibangun menggunakan JavaScript dan C++, terdapat arsitektur serta fungsi dari Google V8 di dalamnya yang berfungsi sebagai *compiler* ditulis dalam C++ dan library Libuv bekerja untuk menangani operasi *asynchronous I/O* dan *main event loop* (Wilson, 2013).

### NestJS

Nest (NestJS) adalah *framework* untuk membangun *server-side applications* Node.js yang efisien. NestJS menggunakan JavaScript progresif yang dibangun dengan mendukung TypeScript secara penuh dan menggabungkan elemen OOP (*Object Oriented Programming*), FP (*Functional Programming*), dan FRP (*Functional Reactive Programming*). Nest menggunakan kerangka kerja Server HTTP *default* Express dan secara opsional dapat dikonfigurasi untuk menggunakan Fastify juga. Nest menyediakan level abstraksi di atas *framework* Node.js (Express / Fastify), tetapi juga mengekspos API-nya secara langsung ke *developer* sehingga memberi kebebasan bagi *developer* untuk menggunakan banyak sekali modul pihak ketiga yang tersedia untuk *platform* yang mendasarinya.

|  |
| --- |
| https://www.digitalkode.com/images/uploads/1_czxaov35etfe545eiugfqq.png |

Gambar 2. 4 NestJS

Sumber: https://www.digitalkode.com/

NestJS memiliki beberapa kelebihan atau fitur unggulan, diantaranya memberikan fleksibilitas dengan memungkinkan untuk penggunaan pustaka lain dengan adanya arsitektur modular *(extensible),* juga merupakan ekosistem yang dapat beradaptasi untuk semua jenis *server-side applications* serta bersifat progresif karena memanfaatkan fitur JavaScript yang terbaru (Mysliwiec, 2017).

### Angular

Angular adalah *framework open-source single-page apps* berbasisTypeScript. Angular dirancang dari penulisan ulang Angular JS oleh Google. Angular dapat dikembangkan di seluruh platform baik *web, mobile web, native mobile,* maupun *native desktop*. Angular melakukan proses *load* dengan cepat melalui *component router* baru, yang memberikan *code-splitting* otomatis sehingga pengguna hanya perlu melakukan *load* kode yang diperlukan untuk me-*render* tampilan yang diminta. Angular dirancang untuk membuat sebuah pembaruan semudah mungkin, sehingga *developer* dapat memanfaatkan perkembangan terbaru dengan *effort* yang minimal.

|  |
| --- |
| https://miro.medium.com/max/700/1*1LQEcTLv8rBn3SixcRcbxw.png |

Gambar 2. 5 Angular

Angular menyediakan beberapa *library* pihak pertama*. Library-library* tersebut berfungsi untuk memperluas fungsionalitas aplikasi sekaligus berfokus pada fitur yang membuat aplikasi yang dikembangkan menjadi lebih unik. *Library* tersebut dirancang untuk diintegrasikan dengan lancar dan diperbarui secara bersamaan dengan kerangka kerja Angular. *Library-library* yang disediakan , antara lain (Angular, 2010) :

1. *Angular Router*, navigasi dan *routing client-side* lanjutan berdasarkan komponen Angular. Mendukung *lazy-loading, nested routes, custom path matching* dan lainnya,
2. *Angular Forms*, sistem yang seragam untuk partisipasi dan validasi *form*.
3. *Angular HttpClient*, HTTP *client* yang kuat yang dapat mendukung komunikasi client -server yang lebih baik.
4. *Angular Animations*, sistem yang kaya untuk menggerakkan animasi berdasarkan status aplikasi.
5. *Angular PWA*, tools untuk membangun *Progressive Web Applications* (*PWA*) termasuk *service worker* dan *web app manifest*.
6. Angular Schematics, *automated scaffolding*, *refactoring*, dan *update tools* yang menyederhanakan pengembangan dalam skala besar.

### Web3JS

Web3js memungkinkan untuk berinteraksi dengan *node* Ethereum lokal atau jarak jauh, menggunakan koneksi HTTP atau IPC. Web3js merupakan pustaka yang memungkinkan untuk melakukan tindakan pengiriman seperti mengirim *ether* dari akun satu ke akun lain, membaca dan menulis *smart contract* dan lain sebagainya.

|  |
| --- |
|  |

Gambar 2. 6 Interaksi Web3.JS dengan Node Ethereum

Web3.js dapat digunakan untuk terhubung ke jaringan Ethereum melalui *node* Ethereum yang memungkinkan akses melalui HTTP. Akses tersebut dapat berupa *node* lokal, *node* yang di-*hosting* oleh penyedia DApp, atau *gateway* publik seperti Infura, yang mengoperasikan titik akses Ethereum gratis. Salah satu cara umum untuk mengintegrasikan aplikasi *browser web* dengan Ethereum adalah dengan menggunakan ekstensi *browser* Metamask dengan kombinasi Web3js (Web3JS, 2016).

## MySQL

MySQL merupakan *software* yang tergolong sebagai DBMS (*Database Management System*) yang bersifat *open source*. *Open source* menyatakan bahwa *software* ini dilengkapi dengan *source code* selain bentuk *executable*-nya atau kode yang dapat dijalankan secara langsung dalam sistem operasi. MySQL memiliki fungsi-fungsi MySQL yang digunakan untuk mengakses *database server* MySQL. Fungsi ini berguna untuk mengantarkan perintah SQL pada PHP menuju ke *server* sehingga perintah tersebut dapat dieksekusi oleh semua *server* MySQL.

Tabel 2. 1 MySQL Function

| **No.** | **Function** | **Kegunaan** |
| --- | --- | --- |
|  | *Mysql\_connect()* | Membuat hubungan ke *database* MySQL yang terdapat pada suatu *host* |
|  | *Mysql\_close()* | Menutup hubungan ke *database MySQL* |
|  | *Mysql\_select\_db()* | Memilih *database* |
|  | *Mysql\_query()* | Mengeksekusi permintaan terhadap sebuah tabel atau sejumlah tabel |
|  | *Mysql\_db\_query()* | Menjalankan suatu permintaan terhadap suatu *database* |
|  | *Mysql\_num\_rows()* | Memperoleh jumlah baris dari suatu hasil permintaan yang menggunakan *SELECT* |
|  | *Mysql\_affected\_rows()* | Memperoleh jumlah baris yang dikenai operasi *INSERT, DELETE, UPDATE* |
|  | *Mysql\_num\_fields()* | Memperoleh jumlah kolom pada suatu hasil permintaan |
|  | *Mysql\_fecth\_row()* | Menghasilkan *array*/baris yang berisi seluruh kolom dari sebuah baris pada suatu himpunan hasil |
|  | *Mysql\_fecth\_array()* | Menghasilkan *array*/baris yang berisi seluruh kolom dari sebuah baris pada suatu himpunan hasil yang akan disimpan dua kali pada *array* hasil |
|  | *Mysql\_fecth\_field()* | Menghasilkan informasi suatu kolom |
|  | *Mysql\_data\_seek()* | Memindahkan pointer pada suatu himpunan hasil supaya menunjuk ke baris tertentu |
|  | *Mysql\_field\_seek()* | Memindahkan pointer pada suatu himpunan hasil supaya menunjuk ke kolom tertentu |
|  | *Mysql\_create\_db()* | Membuat *database MySQL* |
|  | *Mysql\_drop\_db()* | Menghapus *database MySQL* |
|  | *Mysql\_list\_dbs()* | Menghasilkan daftar *database MySQL* |
|  | *Mysql\_list\_tables()* | Memperoleh daftar nama tabel dalam suatu *database* |
|  | *Mysql\_list\_fields()* | Memperoleh daftar nama kolom dalam suatu *database* |
|  | *Mysql\_fetch\_assoc()* | Mendapatkan array baris dari suatu *recordset* |
|  | *Mysql\_fetch\_lengths()* | Mendapatkan panjang baris pada setiap isi *field* |
|  | *Mysql\_fetch\_object()* | Menghasilkan baris dari *recordset* sebagai sebuah objek |
|  | *Mysql\_field\_len()* | Mendapatkan informasi panjang maksimum *field* dalam sebuah *recorset* |
|  | *Mysql\_field\_name()* | Mendapatkan informasi nama *field* dalam *recordset* |
|  | *Mysql\_ping()* | Memeriksa koneksi *server* dan akan mencoba untuk melakukan koneksi ulang jika koneksi terputus |

Tabel 2.1 merupakan fungsi-fungsi dalam MySQL yang dapat digunakan untuk mengantarkan perintah SQL pada PHP menuju ke *server* sehingga perintah tersebut dapat dieksekusi oleh semua *server* MySQL.

Selain fungsi-fungsinya, MySQL juga memiliki beberapa keunggulan, seperti dapat berjalan stabil pada berbagai sistem operasi seperti Windows, Linux, FreeBSD, Mac Os X Server, Solaris, Amiga, dan masih banyak lainnya. MySQL didistribusikan sebagai perangkat lunak sumber terbuka, dibawah lisensi GPL sehingga dapat digunakan secara gratis serta dapat digunakan oleh beberapa pengguna dalam waktu yang bersamaan tanpa mengalami masalah atau konflik. MySQL memiliki kecepatan yang tinggi dalam menangani *query* sederhana, dengan kata lain dapat memproses lebih banyak SQL per satuan waktu. MySQL memiliki ragam tipe data yang sangat kaya, seperti *signed / unsigned integer, float, double, char, text, date, timestamp*, dan lain-lain. MySQL memiliki antar muka (*interface*) terhadap berbagai aplikasi dan bahasa pemrograman dengan menggunakan fungsi API (*Application Programming Interface*) (Kadir, 2008).

## JSON

JSON (JavaScript Object Notation) adalah format pertukaran data yang ringan, mudah dibaca dan ditulis oleh manusia, serta mudah diterjemahkan dan dibuat (*generate*) oleh komputer. Format ini dibuat berdasarkan bagian dari bahasa pemrograman JavaScript, Standar ECMA-262 Edisi ke-3 Desember 1999. JSON merupakan format teks yang tidak bergantung pada bahasa pemrograman apapun karena menggunakan gaya bahasa yang umum digunakan oleh *programmer* keluarga C termasuk C, C++, C#, Java, JavaScript, Perl, Python dan lainnya (Derizal, 2011).

## Google Cloud Platform

Google Cloud Platform merupakan layanan *public cloud computing* dari Google yang terdiri dari beragam layanan. *Platform* dari Google ini menyediakan beragam layanan *hosting* mulai dari komputasi, *storage* dan *aplication development* yang berjalan pada *hardware* Google. Google Cloud Platform Service dapat diakses oleh pengembang *software, administrator cloud* dan profesional IT lainnya menggunakan internet publik atau melalui koneksi jaringan *dedicated* (Google, 2021).

### Compute Engine

Google Compute Engine memungkinkan untuk menjalankan beban kerja komputasi skala besar dengan infrastruktur yang sama yang menjalankan Google Search, Gmail dan Ads. Pengguna dapat meluncurkan *virtual machines* sesuai permintaan, mengelola konektivitas jaringan menggunakan solusi jaringan yang sederhana namun fleksibel, dan mengakses berbagai alternatif penyimpanan data dari *virtual machines*. Fitur-fitur Google Compute Engine antara lain (Google, 2021) :

1. *Full Virtual Machines:* Mesin virtual yang di-*hosting* kernel yang menjalankan Ubuntu atau CentOs. Meluncurkan 1, 2, 4, atau 8 *virtual core instances* dengan memori 3.75 GB per *virtual core*.
2. *Flexible Storage:* menawarkan opsi penyimpanan yang berbeda untuk memenuhi berbagai kebutuhan.
3. *Flexible networking:* menawarkan solusi jaringan yang memudahkan untuk menghubungkan *virtual machines* satu sama lain dan ke Internet.
4. *Open tooling:* menawarkan UI sederhana dan *command-line tooling* untuk mengonfigurasi dan meluncurkan *virtual machines*.

# BAB III METODOLOGI DAN PERANCANGAN SISTEM

BAB III ini memuat metode yang digunakan dalam penelitian beserta dengan proses pembuatan laporan yang meliputi tempat dan waktu penelitian, sumber data dan metode pengumpulan, instrument perancangan, dan gambaran umum sistem.

## Tempat dan Waktu Penelitian

Penelitian ini bertempat di Kampus Bukit Universitas Udayana, Fakultas Teknik, Program Studi Teknologi Informasi yang berlokasi di Jalan Kampus Bukit UNUD Jimbaran*,* Kabupaten Badung, Bali. Kampus Bukit Universitas Udayana dipilih karena memiliki semua aspek pendukung agar penelitian dapat berjalan dengan baik. Penelitian dilaksanakan pada semester genap tahun ajaran 2019-2020 yaitu antara bulan Januari sampai dengan bulan Juni dan semester ganjil tahun ajaran 2020-2021 yaitu antara bulan Juli sampai dengan bulan Desember.

## Metode Penelitian

Metode penelitian yang digunakan pada pembuatan sistem *e-voting* ini adalah *Agile Software Development Methods.* Metode *Agile* pertama kali diperkenalkan oleh Kent Beck bersama dengan 16 rekannya. Metode *agile* merupakan sekumpulan metode pengembangan perangkat lunak yang berbasis pada pengembangan iteratif yang dilakukan dengan kolaborasi yang terorganisir. Metode *agile* berfokus pada perkembangan yang cepat, perangkat lunak yang dirilis bertahap, mengurangi *overhead* proses, dan menghasilkan kode berkualitas tinggi dan pada proses perkembangannya melibatkan pelanggannya secara langsung (Sommerville, 2011).

|  |
| --- |
| https://pelajarindo.com/wp-content/uploads/2018/08/Pengertian-Metode-Agile.png |

Gambar 3. 1 *Agile Software Development Method*

Gambar 3.1 merupakan gambaran dari metode *agile* yang akan digunakan dalam pengembangan sistem *e-voting* berbasis *ethereum smart contract*. *Agile* sendiri merupakan gabungan dari metode *incremental* dan *iterative*. Dibandingkan dengan metode *waterfall*, *agile* tidak memiliki fase-fase yang paten. *Agile* berproses iteratif dengan perputaran yang pendek. Kebutuhan direncananakan, diimplementasikan, diuji, dan dievaluasi secara berulang.

Metode *agile* masih terbagi menjadi beberapa jenis bagian, diantaranya *Adaptive Software Development* (ASD), *Agile Modelling* (AM), *Crystal*, *Dynamic System Development Method* (DSDM), *Extreme Programming* (XP), *Feature Driven Development* (FDD), *Rational Unified Process*, dan *Scrum Methodology*. Jenis *agile* yang paling sering digunakan adalah *Adaptive Software Development* (ASD), *Dynamic System Development Method* (DSDM), *Extreme Programming* (XP), dan *Scrum* (Pressman, 2010).

Penelitian ini akan menggunakan jenis metode *Scrum*. Walaupun sebenarnya metode ini biasanya digunakan secara tim, namun secara khusus tidak ada larangan untuk menggunakannya secara perorangan. Metode *scrum* membagi proses *development* menjadi beberapa *sprint*. *Sprint* ini akan bertindak sebagai *milestone* dalam pembuatan *software.* Berikut ini merupakan beberapa tahapan dalam *Scrum.*

### Backlog

Tahap ini melakukan proses menyusun rincian prioritas pada fitur-fitur yang akan dibangun pada sistem *e-voting* yang akan dikembangkan. Umumnya, tahapan ini bertujuan untuk merancang pekerajaan-pekerjaan yang akan dilakukan berdasarkan permintaan atau kebutuhan *user*.

Proses-proses yang akan dilakukan pada perancangan sistem *e-voting* adalah perancangan *database*, perancangan *API* *backend,* integrasi dengan *ethereum node,* dan perancangan *frontend.*  Isi pada masing-masing proses secara rinci dapat ditambahkan setiap memulai siklus pengembangan karena satu proses dan lainnya tidak diselesaikan secara langsung dalam suatu waktu sehingga dalam setiap proses dapat terjadi perubahan dan penambahan lebih lanjut.

### Sprints

Tahapan selanjutnya yaitu memasukan pekerjaan-pekerjaan yang harus dilakukan dan menyusun prioritasnya ke dalam *sprints.* Proses ini menyusun kegiatan yang akan dilakukan untuk memenuhi kebutuhan dan ditetapkan dalam *backlog* dengan durasi realisasi selama hari kerja yang ditentukan yaitu selama 2 minggu. Setiap sprint mengerjakan hampir keseluruhan proses yang disebutkan dalam *backlog* atau paling sedikit 3 dari 4 proses. Prioritas pekerjaan yang harus dikerjakan sesuai waktu yang ditentukan adalah perancangan *database*, perancangan *API* *backend,* integrasi dengan *ethereum node,* sedangkan untuk perancangan *frontend,* di awal pengembangan masih belum mendapat prioritas utama, namun akan menjadi fokus setelah proses-proses lainnya mencapai hasil dengan persentase yang sudah lebih besar.

### Scrum Meeting

Tahap ini dilakukan dengan menganalisis dari sisi pengembang untuk mengetahui seberapa banyak kemajuan dari kegiatan pengembangan sistem yang telah dilakukan atau dicapai. Tahap ini dilakukan dengan pengujian jenis *automated testing* yaitu *unit testing* dan *e2e testing* terhadap 10 *file* dengan masing-masing *file* terdiri atas kurang lebih 5 skenario pengujian*.*

### Demos

Langkah selanjutnya adalah memperlihatkan fitur-fitur *software* yang telah dihasilkan dalam proses pengembangan untuk dievaluasi oleh pengguna sesuai dengan waktu yang telah ditentukan. Tahapan ini dalam pengembangan sistem *e-voting* dibantu oleh dosen pembimbing 1 dan dosen pembimbing 2 tugas akhir sebagai pihak yang memberi masukan dan saran atas pengembangan yang telah dilakukan untuk kemudian dilakukan evaluasi kembali.

Sementara itu, di dalam setiap iterasi kegiatan pengembangan sistem yang telah dijelaskan sebelumnya, terdapat beberapa rangkaian kegiatan di dalamnya, yaitu sebagai berikut.

1. Analisa Kebutuhan Sistem: Asesmen terhadap pengguna untuk menggali secara detail *software requirement* yang dibutuhkan oleh pengguna.
2. Desain: perancangan sistem, mulai dari desain arsitektur sistem, desain proses bisnis, desain *database*, hingga desain *user interface*.
3. *Code Generation*:penulisan kode program dan manajemen *database*
4. *Testing*: proses meminimalisir kesalahan (*error*) dan memastikan *output* yang dihasilkan telah sesuai dengan *user requirement.*
5. *Support*: proses menindaklanjuti perubahan yang diperlukan setelah proses *testing* dan evaluasi sesuai dengan kebutuhan pengguna.

## Gambaran Umum Sistem

Sistem Voting Elektronik berbasis *Ethereum Smart Contract* merupakan sistem yang digunakan sebagai sarana pemilihan elektronik dengan menerapkan teknologi *blockchain*. Gambar 3.2 merupakan gambaran umum arsitektur sistem *e-voting* berbasis *ethereum smart contract*. Gambaran umum arsitektur teknologi merupakan bagan yang menjelaskan alur kerja teknologi yang digunakan secara menyeluruh secara umum.

|  |
| --- |
|  |

Gambar 3. 2 Gambaran Umum Sistem

Gambar 3.2 merupakan gambaran umum dari Sistem Voting Elektronik berbasis *Ethereum Smart Contract*. Semua kebutuhan komputasi yaitu Virtual Machine menggunakan penyedia Google Cloud. Terdapat empat Virtual Machine yang digunakan dalam sistem. Masing-masing VM menggunakan OS Ubuntu 18.04. Sebuah VM digunakan untuk menjalankan RDBMS MySQL, dua buah VM untuk menjalankan Openethereum dan yang terakhir digunakan untuk menjalankan dua proses node untuk aplikasi backend dan frontend.

Pertama *super admin* akan membuat akun untuk *election authority*. *Election authority* akan membuat membuat eleksi dan menambahkan kandidat pada eleksi. Eleksi akan di *review* oleh *super admin* apakah diijinkan untuk di-*deploy* ke *blockchain*. Jika eleksi sudah di-*deploy* maka *voter* dapat melakukan pemilihan dan data akan terekam pada *blockchain*. Kemudian eleksi akan dihentikan oleh *election authority* dan *voter* dapat melihat hasil dari eleksi tersebut.

### Use Case Diagram

Use case diagram merupakan representasi interaksi *user* dengan sistem dan menggambarkan spesifikasi dari *use case*. *Use case* untuk sistem *e-voting* berbasis *Ethereum Smart Contract* ditunjukkan oleh Gambar 3.3.

|  |
| --- |
| C:\Users\sarah\AppData\Local\Microsoft\Windows\INetCache\Content.Word\usecase.png |

Gambar 3. 3 *Use Case Diagram*

Gambar 3.3 menunjukkan *use case* dari sistem *e-voting* berbasis *Ethereum Smart Contract*. *Use case* tersebut menggambarkan interaksi pengguna terhadap sistem *e-voting* dan interaksi antara satu elemen dengan elemen lainnya. *Use case* aplikasi sistem *e-voting* memiliki 3 aktor, diantaranya *super admin, election authority* dan *voter*.

Masing-masing aktor memiliki peran dan akses yang berbeda-beda. *Super admin* dapat melakukan penambahan atau mendaftarkan *election authority* ke dalam sistem, melakukan proses *send ether* danproses *deploy* atau aktivasi *election* sehingga dapat digunakan, serta melihat hasil *election*. *Election authority* dapat melakukan pembuatan *election* baru, menambahkan kandidat dalam *election* yang dibuat, menentukan awal dan berakhirnya *election,* serta melihat hasil *election. Voter* dapat melakukan pendaftaran dalam setiap *election* yang diikuti dan melakukan proses *vote* dalam *election* yang dipilih, serta melihat hasil *election.*

### Rancangan Alur Sistem

Rancangan alur penggunaan aplikasi sistem *e-voting* berbasis *Ethereum Smart Contract* digunakan sebagai acuan untuk membuat antarmuka dari aplikasi.

1. Rancangan Alur Sistem *(Super Admin)*

Aplikasi sistem *e-voting* memiliki 3 jenis *user* yang memiliki peran dan akses yang berbeda-beda. Jenis *user* yang pertama adalah *super admin*. Rancangan alur sistem dengan *super admin* sebagai *user* dapat dilihat pada Gambar 3.4.

|  |
| --- |
|  |

Gambar 3. 4 Rancangan Alur Sistem *(Super Admin)*

Gambar 3.4 menggambarkan rancangan alur keseluruhan sistem dengan *super admin* sebagai *user*. Pertama-tama, *super admin* harus *login* terlebih dahulu ke dalam sistem. Setelah berhasil *login, super admin* dapat melakukan pembuatan akun bagi *election authority.* Apabila terdapat *election* baru yang siap di­-*deploy,* maka *super admin* bertugas melakukan proses *deploy* ke *blockchain.*

1. Rancangan Alur Sistem *(Election Authority)*

Jenis *user* selanjutnya adalah *election authority,* yaitu *user* yang bertanggung jawab untuk membuat dan menangani satu atau lebih *election.* Rancangan alur sistem dengan *election authority* sebagai *user* dapat dilihat pada Gambar 3.5.

|  |
| --- |
| C:\Users\sarah\Downloads\Telegram Desktop\flowchart-election-authority.png |

Gambar 3. 5 Rancangan Alur Sistem *(Election Authority)*

Gambar 3.5 menggambarkan rancangan alur keseluruhan sistem dengan *election authority* sebagai *user.* Alur sistem diawali dengan proses *login* oleh *election authority* menggunakan akun yang telah didaftarkan atau dibuat oleh *super admin* sebelumnya.Setelah berhasil *login,* maka *election authority* dapat melakukan proses pembuatan *election* baru, diikuti dengan peambahan daftar kandidatnya. Setelah itu, apabila election yang dibuat telah di-*deploy* oleh *super admin,* maka *election authority* dapat memulai *election.* Namun, apabila *election* belum di-*deploy,* maka *election authority* harus menunggu sampai *election* berhasil di­-*deploy* oleh *super admin* untuk dapat memulai *election.*

1. Rancangan Alur Sistem *Voter*

Jenis *user* yang terakhir adalah *voter,* yaitu *user* yang memiliki hak suara dan berhak memilih dalam satu atau lebih *election.* Rancangan alur sistem dengan *voter* sebagai *user* dapat dilihat pada Gambar 3.6.

|  |
| --- |
|  |

Gambar 3. 6 Rancangan Alur Sistem *(Voter )*

Gambar 3.6 menggambarkan rancangan alur keseluruhan sistem dengan *voter* sebagai *user.* Langkah pertama yang harus dilakukan oleh *voter* adalah *login* ke dalam sistem. Setelah berhasil *login,* maka *voter* dapat mendaftar ke dalam *election* yang akan diikuti. Pendaftaran *voter* dalam *election* harus terlebih dahulu disetujui untuk selanjutnya dapat melihat daftar kandidat dalam *election,* namun apabila pendaftaran ditolak, maka *voter* harus melakukan pendaftaran ulang sampai pendaftaran diterima untuk dapat mengikuti *election* tersebut. Proses pemungutan suara atau *vote* hanya dapat dilakukan oleh *voter* apabila *election* telah dimulai.

1. Rancangan Alur Proses *Login*

Proses *login* dapat dilakukan oleh 3 aktor yang terlibat dalam mengakses sistem. Rancangan alur untuk proses *login* pada sistem *e-voting* dapat dilihat pada Gambar 3.7.

|  |
| --- |
| C:\Users\sarah\AppData\Local\Microsoft\Windows\INetCache\Content.Word\flowchart-login .png |

Gambar 3. 7 Rancangan Alur Proses *Login*

Gambar 3.7 memperlihatkan aktivitas untuk melakukan proses *login* untuk masuk atau mengakses sistem. Proses *login* juga menentukan hak akses dari masing-masing aktor yang terlibat. Setelah melakukan pengecekan data *login* yang dimasukkan maka dilakukan pengecekan terhadap *role* dari *user* yang akan *login.* Apabila dalam proses pengecekan tidak ada kesalahan, maka *user* akan dibawa menuju halaman sesuai dengan *user role.* Apabila terdapat kesalahan, maka *user* akan diminta memasukkan data *login* kembali.

1. Rancangan Alur Penambahan *Election Authority*

Rancangan alur untuk proses penambahan *election authority* pada sistem *e-voting* dapat dilihat pada Gambar 3.8.

|  |
| --- |
| C:\Users\sarah\AppData\Local\Microsoft\Windows\INetCache\Content.Word\super-admin_create-ea.png |

Gambar 3. 8 Rancangan Alur Penambahan *Election Authority*

Gambar 3.8 memperlihatkan proses penambahan atau pembuatan *election authority* baru oleh *super admin.* Data yang dimasukkan untuk pembuatan *election authority* adalah nama, *usernme* dan *password. Username* harus bersifat *unique* atau belum pernah digunakan sebelumnya.

1. Rancangan Alur Pembuatan *Election*

Rancangan alur untuk proses pembuatan *election* baru pada sistem *e-voting* dapat dilihat pada Gambar 3.9.

|  |
| --- |
| C:\Users\sarah\AppData\Local\Microsoft\Windows\INetCache\Content.Word\election-authority_create-election.png |

Gambar 3. 9 Rancangan AlurPembuatan *Election* Baru

Gambar 3.9 memperlihatkan aktivitas untuk melakukan penambahan atau pembuatan *election* baru. *Election authority* yang bertugas melakukan pembuatan *election* baru meng-*input*-kan nama*,* deskripsi, serta tanggal berlangsungnya pemilihan. Setelah proses pembuatan *election,* maka *election* baru berhasil dibuat.

1. Rancangan Alur Tambah Kandidat

Rancangan alur untuk proses penambahan kandidat yang dapat dipilih dalam sebuah *election* pada sistem *e-voting* dapat dilihat pada Gambar 3.10.

|  |
| --- |
| C:\Users\sarah\AppData\Local\Microsoft\Windows\INetCache\Content.Word\election-authority_add-candidate.png |

Gambar 3. 10 Rancangan AlurPenambahan Kandidat

Gambar 3.10 memperlihatkan aktivitas untuk melakukan proses penambahan kandidat yang dapat dipilih dalam sebuah *election*. Sebelum melakukan penambahan kandidat, *election authority* harus terlebih dahulu membuat *election. Election* yang telah berhasil dibuat kemudian dapat dipilih untuk melakukan penambahan kandidat. *Election authority* memasukkan data nama, visi, misi dan pengalaman dari kandidat. Proses penambahan kandidat dapat dilakukan secara berulang sebanyak jumlah kandidat dalam *election* yang dipilih.

1. Rancangan Alur *Deploy Election*

Rancangan alur untuk proses aktivasi *election* yang telah dibuat sehingga dapat digunakan atau *deploy election* dapat dilihat pada Gambar 3.11.

|  |
| --- |
| C:\Users\sarah\AppData\Local\Microsoft\Windows\INetCache\Content.Word\super-admin_deploy-election.png |

Gambar 3. 11 Rancangan Alur *Deploy Election*

Gambar 3.11 memperlihatkan aktivitas untuk melakukan proses mengaktifkan *election* yang telah dibuat oleh *election authority* sebelumnya atau proses membawa *smart contract* ke *blockchain* sehingga dapat digunakan. Setelah *election* yang akan di-*deploy* dipilih, maka akan dilakukan proses pengiriman *ether* dari *super admin* ke *wallet address election authority.* Selanjutnya dilakukan proses *deploy smart contract* ke *private blockchain* dan penentuan kandidat di *smart contract* bedasarkan data yang tersimpan di basis data. Setelah semua proses selesai dilakukan maka *smart contract* telah berhasil di-*deploy* dan sudah dapat digunakan.

1. Rancangan Alur Registrasi *Voter*

Sebelum dapat melakukan proses *voting, s*etiap *voter* harus terdaftar pada sistem terlebih dahulu. Rancangan alur untuk proses pendaftaran *voter* dapat dilihat pada Gambar 3.12.

|  |
| --- |
| C:\Users\sarah\AppData\Local\Microsoft\Windows\INetCache\Content.Word\umum-register-voter.png |

Gambar 3. 12 Rancangan Alur Registrasi *Voter*

Gambar 3.12 memperlihatkan aktivitas untuk melakukan proses pendaftaran masing-masing *voter* dalam sistem *e-voting*. *Voter* memasukkan *username* yang bersifat unik dan *password* untuk melakukan proses pembuatan akun yang terdaftar dalam sistem.

1. Rancangan Alur Pendaftaran *Voter* dalam *Election*

Setiap *voter* yang telah terdaftar di sistem akan melakukan *voting* dan juga harus terdaftar pada masing-masing *election* yang akan diikuti. Rancangan alur untuk proses pendaftaran *voter* dapat dilihat pada Gambar 3.13.

|  |
| --- |
| C:\Users\sarah\AppData\Local\Microsoft\Windows\INetCache\Content.Word\voter_voter-register-to-election.png |

Gambar 3. 13 Rancangan Alur Pendaftaran *Voter* dalam *Election*

Gambar 3.13 memperlihatkan aktivitas untuk melakukan proses pendaftaran masing-masing *voter* dalam setiap *election* yang diikuti. Setelah melakukan pemilihan *election* yang diikuti, maka *election authority* akan memverifikasi apakah *voter* tersebut memiliki hak suara atau tidak dalam *election* yang dipilih.

1. Rancangan Alur Proses *Vote*

Rancangan alur untuk pemberian suara atau *vote* oleh setiap *voter* dalam sebuah *election* pada sistem *e-voting* dapat dilihat pada Gambar 3.14.

|  |
| --- |
| C:\Users\sarah\AppData\Local\Microsoft\Windows\INetCache\Content.Word\voter_voter-vote.png |

Gambar 3. 14 Rancangan Alur Proses *Vote*

Gambar 3.14 memperlihatkan aktivitas untuk melakukan proses *vote* oleh masing-masing *voter. Voter* terlebih dahulu melakukan pemilihan *election* dan selanjutnya memilih kandidat yang akan di *vote.* Setelah itu dilakukan proses pengiriman *ether* dari *super admin* ke *wallet address voter* dilanjutkan dengan proses pemanggilan fungsi *vote* pada *smart contract* oleh *voter.* Apabila semua proses telah selesai dilakukan maka suara dari *voter* telah berhasil terekam di *blockchain.*

## Rancangan Basis Data

Perancangan basis data merupakan suatu langkah dalam merancang basis data yang akan digunakan pada sistem. Perancangan basis data digunakan sebagai pendekatan struktur dengan menggunakan prosedur, teknik, alat serta bantuan dokumen untuk membantu dan memudahkan dalam proses perancangan.

### Implementasi Basis Data

Implementasi basis data diambil berdasarkan perancangan basis data yang telah dibuat, secara fisik, implementasi basis data diimplementasikan menggunakan perangkat lunak MySQL. Struktur tabel basis data dapat dilihat pada Gambar 3.15.

|  |
| --- |
| db_simvoni |

Gambar 3. 15 Implementasi Basis Data

Gambar 3.15 merupakan implementasi basis data dari *e-voting* berbasis *Ethereum Smart Contract*. Basis data tersebut digunakan sebagai media penyimpanan informasi data *user*, *election* dan *candidate*.

### Struktur Data Tabel

Basis data merupakan kumpulan data yang disatukan di dalam kumpulan tabel. Struktur data dari masing-masing tabel dalam perancangan basis data dijelaskan sebagai berikut.

Tabel user diberi nama tabel ref\_user. Tabel ini menyimpan seluruh data dari masing-masing user yang terdaftar dalam sistem ­*e-voting.* Struktur data tabel ref\_user dapat dilihat pada Tabel 3.1.

Tabel 3. 1 Struktur Data Tabel ref\_user

| Nama Field | Tipe Data | Panjang | Keterangan |
| --- | --- | --- | --- |
| user\_id | int |  | Primary key |
| user\_nama | varchar | 255 |  |
| user\_username | varchar | 255 |  |
| user\_password | varchar | 255 |  |
| user\_wallet\_address | varchar | 255 |  |
| user\_role\_id | Int |  | Foreign key |
| user\_login\_at | datetime |  |  |

Tabel 3.1 merupakan struktur data dari tabel ref\_user yang memiliki user\_id sebagai *primary key* beserta dengan *field* user\_nama, user\_username, user\_password, user\_wallet\_address, user\_role\_id, dan user\_login\_at.

Tabel selanjutnya adalah tabel ref\_user\_role. Tabel ini menyimpan data dari *user role* yang ada dalam sistem ­*e-voting.* Struktur data tabel ref\_user\_role dapat dilihat pada Tabel 3.2.

Tabel 3. 2 Struktur Data Tabel ref\_user\_role

| Nama Field | Tipe Data | Panjang | Keterangan |
| --- | --- | --- | --- |
| user\_role\_id | int |  | Primary key |
| user\_role\_nama | varchar | 255 |  |

Tabel 3.2 merupakan struktur data dari tabel ref\_user\_role yang memiliki user\_role\_id sebagai *primary key* beserta dengan *field* user\_role\_nama.

Tabel selanjutnya adalah tabel ta\_candidate. Tabel ini menyimpan seluruh data dari masing-masing kandidatyang terdaftar dalam sistem ­*e-voting.* Struktur data tabel ta\_candidate dapat dilihat pada Tabel 3.3.

Tabel 3. 3 Struktur Data Tabel ta\_candidate

| Nama Field | Tipe Data | Panjang | Keterangan |
| --- | --- | --- | --- |
| candidate\_id | int |  | Primary key |
| candidate\_name | varchar | 255 |  |
| candidate\_election\_id | int | 255 | Foreign key |
| candidate\_visi | varchar | 255 |  |

Tabel 3.3 merupakan struktur data dari tabel ta\_candidate yang memiliki candidate\_id sebagai *primary key* beserta dengan *field* candidate\_name, candidate\_election\_id, dan candidate\_visi.

Tabel selanjutnya adalah tabel ta\_misi. Tabel ini menyimpan seluruh data misi dari masing-masing kandidatyang terdaftar dalam sistem ­*e-voting.* Struktur data tabel ta\_misi dapat dilihat pada Tabel 3.4.

Tabel 3. 4 Struktur Data Tabel ta\_misi

| Nama Field | Tipe Data | Panjang | Keterangan |
| --- | --- | --- | --- |
| misi\_id | int |  | Primary key |
| misi\_deskripsi | varchar | 255 |  |
| misi\_candidate\_id | int | 255 | Foreign key |

Tabel 3.4 merupakan struktur data dari tabel ta\_misi yang memiliki misi\_id sebagai *primary key* beserta dengan *field* misi\_deskripsi dan misi\_candidate\_id.

Tabel selanjutnya adalah tabel ta\_pengalaman. Tabel ini menyimpan seluruh data pengalaman dari masing-masing kandidatyang terdaftar dalam sistem ­*e-voting.* Struktur data tabel ta\_pengalaman dapat dilihat pada Tabel 3.5.

Tabel 3. 5 Struktur Data Tabel ta\_pengalaman

| Nama Field | Tipe Data | Panjang | Keterangan |
| --- | --- | --- | --- |
| pengalaman\_id | int |  | Primary key |
| pengalaman\_deskripsi | varchar | 255 |  |
| pengalaman\_candidate\_id | int | 255 | Foreign key |

Tabel 3.5 merupakan struktur data dari tabel ta\_pengalaman yang memiliki pengalaman\_id sebagai *primary key* beserta dengan *field* pengalaman \_deskripsi dan pengalaman \_candidate\_id.

Tabel selanjutnya adalah tabel ta\_election. Tabel ini menyimpan seluruh data *election* yang terdaftar dalam sistem ­*e-voting.* Struktur data tabel ta\_election dapat dilihat pada Tabel 3.6.

Tabel 3. 6 Struktur Data Tabel ta\_election

| Nama Field | Tipe Data | Panjang | Keterangan |
| --- | --- | --- | --- |
| election\_id | int |  | Primary key |
| election\_name | varchar | 255 |  |
| election\_description | varchar | 255 |  |
| election\_authority | int |  | Foreign key |
| election\_status | int |  | Foreign key |
| election\_start | date |  |  |
| election\_end | date |  |  |
| election\_contract\_address | varchar | 255 |  |

Tabel 3.6 merupakan struktur data dari tabel ta\_election yang memiliki election\_id sebagai *primary key* beserta dengan *field* election\_name, election\_description, election\_authority, election\_status, election\_start, election\_end, dan election\_contract\_address

Tabel selanjutnya adalah tabel ref\_election\_status. Tabel ini menyimpan seluruh data *election status* yang terdaftar dalam sistem ­*e-voting.* Struktur data tabel ref\_election\_status dapat dilihat pada Tabel 3.7.

Tabel 3. 7 Struktur Data Tabel ref\_election\_status

| Nama Field | Tipe Data | Panjang | Keterangan |
| --- | --- | --- | --- |
| election\_status\_id | int |  | Primary key |
| election\_status | varchar | 255 |  |

Tabel 3.7 merupakan struktur data dari tabel ref\_election\_status yang memiliki election\_status\_id sebagai *primary key* beserta dengan *field* election\_status.

## Bahasa Pemrograman

Implementasi Sistem Voting Elektronik Berbasis *Ethereum Smart Contract* merupakan aplikasi berbasis web. Aplikasi ini dibangun dengan bahasa pemrograman Typescript untuk *frontend* dan *backend* dan Solidity untuk membuat Smart Contract. Adapun *database* yang digunakan adalah *database* MySQL.

## Rancangan Antarmuka Aplikasi

# BAB IV PENGUJIAN DAN ANALISA HASIL

BAB IV menjelaskan hasil dari penelitian ini yaitu berupa hasil pengujian aplikasi, dan analisa dari aplikasi yang telah dikembangkan serta survei terhadap perangkat lunak yang telah dibuat dan implementasinya ke dalam perangkat keras yaitu *smartphone* berbasis Android.

## Alat Penelitian Aplikasi

### Kebutuhan Perangkat Lunak Implementasi Aplikasi

### Kebutuhan Perangkat Keras Implementasi Aplikasi

## Konfigurasi Node Ethereum

### Genesis Block

### Konfigurasi Node

### Menghubungkan Node

## Implementasi Desain Antarmuka

### Membuat Eleksi

### Deploy Eleksi

### Memulai Eleksi

### Vote

### Menghentikan Eleksi

## Implementasi Rancangan API

### Membuat Eleksi

### Deploy Eleksi

### Memulai Eleksi

### Vote

### Menghentikan Eleksi

## Pengujian Sistem Voting Elektronik

### Pengujian API Aplikasi

1. Pengujian API Pembuatan Eleksi
2. Pengujian API Deploy Eleksi
3. Pengujian API Mulai Eleksi
4. Pengujian API Vote
5. Pengujian API Hentikan Eleksi

### Pengujian Integritas Data Blockchain

# BAB V PENUTUP

BAB V membahas mengenai kesimpulan yang mengacu pada rumusan masalah dan tujuan penelitian beserta saran yang diberikan peneliti untuk kepentingan pengembangan aplikasi selanjutnya.

## Kesimpulan

## Saran

# DAFTAR PUSTAKA

Adhi, R. A. & Harjono, 2014. Rancang Bangun Sistem Informasi E-Voting Berbasis SMS. *JUITA,* III(2), pp. 85-93.

Angular, 2010. *Angular.*[Online] Available at: https://angular.io/ [Accessed 31 March 2021].

Ardilla, R., 2018. Rancang Bangun Sistem E – Voting Dengan Metode Enkripsi Blockchain Di Kota Mojokerto. *Repository Universitas Islam Majapahit.*

Code, V. S., 2021. *Visual Studio Code.* [Online] Available at: https://code.visualstudio.com [Accessed 31 March 2021].

Copes, F., 2019. *The Next.js Handbook.* s.l.:s.n.

Derizal, 2011. Panduan Lengkap PHP, Ajax, jQuery. *PHP Ajax Javascript jQuery Tutorial Indonesia,* pp. 27-39.

Google, C., 2021. *Google Cloud.* [Online] Available at: https://cloud.google.com/ [Accessed 31 March 2021].

Johari, R. et al., 2020. SEVA: Secure E-Voting Application in Cyber Physical System. *Cyber-Physical Systems,* pp. 1-31.

Kadir, A., 2008. *Tuntunan Praktis Belajar Database Menggunakan MySQL.* Yogyakarta: Andi Offset.

Kurnia Hu, S. D., Palit, H. N. & Handojo, A., 2019. Implementasi Blockchain: Studi Kasus e-Voting. *Jurnal Infra,* VII(1).

Mysliwiec, K., 2017. *NestJS.* [Online] Available at: https://nestjs.com/ [Accessed 31 March 2021].

Pierro, M. D., 2017. What Is the Blockchain?. *Computing in Science & Engineering,* Volume 19, pp. 92-95.

Pressman, R., 2010. *Software Engineering : a practitioner’s approach.* New York: McGraw - Hill.

Rahardja, U., Aini, Q., Yusup, M. & Edliyanti, A., 2020. Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce. *Journal of Computer Engineering System and Science,* V(1), pp. 28--32.

Ridwan, M., Arifin, Z. & Yulianto, 2016. Rancang Bangun E-Voting Menggunakan Keamanan RSA. *Jurnal Informatika Mulawarman.*

Setia, T. E. H. & Susanto, A., 2019. Smart Contract Blockchain pada E-Voting. *Jurnal Informatika Upgris ,* V(2), pp. 188-191.

Sommerville, I., 2011. *Software Engineering.* 9 ed. United States of America: Pearson Education Inc., publishing as Addison-Wesley.

Web3JS, 2016. *web3.js.* [Online] Available at: https://web3js.readthedocs.io/  
[Accessed 31 March 2021].

Wilson, J. R., 2013. *Node.js the Right Way.* 1st ed. United States of America: The Pragmatic Programmers, LLC..