KATA PENGANTAR

DAFTAR ISI

[KATA PENGANTAR i](#_Toc178103642)

[DAFTAR ISI ii](#_Toc178103643)

[DAFTAR GAMBAR iii](#_Toc178103644)

[DAFTAR TABEL iv](#_Toc178103645)

[DAFTAR ISTILAH vi](#_Toc178103646)

[DAFTAR LAMPIRAN vii](#_Toc178103647)

[BAB I PENDAHULUAN 8](#_Toc178103648)

[1.1. Latar Belakang 8](#_Toc178103649)

[1.2. Rumusan Masalah 11](#_Toc178103650)

[1.3. Tujuan Penelitian 11](#_Toc178103651)

[1.4. Manfaat Penelitian 11](#_Toc178103652)

[1.5. Batasan Masalah 12](#_Toc178103653)

[1.6. Kerangka Pemikiran Penelitian 12](#_Toc178103654)

[1.7. Sistematika Penulisan 13](#_Toc178103655)

[BAB II KAJIAN LITERATUR 15](#_Toc178103656)

[2.1. *State of the Art* 15](#_Toc178103657)

[2.2. Dasar Teori 21](#_Toc178103658)

[2.2.1. Blockchain 21](#_Toc178103659)

[2.2.2. Pemilihan Elektronik 23](#_Toc178103660)

[2.2.3. Ethereum 24](#_Toc178103661)

[2.2.4. *Smart Contract* 26](#_Toc178103662)

[2.2.5. *Solidity* 27](#_Toc178103663)

[BAB III METODE PENELITIAN 29](#_Toc178103664)

[3.1. *Plan* (Perencanaan) 29](#_Toc178103665)

[3.2. *Design* (Desain) 29](#_Toc178103666)

[3.3. *Develop* (Pengembangan) 30](#_Toc178103667)

[3.4. *Test* 30](#_Toc178103668)

[3.5. *Deploy* 30](#_Toc178103669)

[BAB IV HASIL DAN PEMBAHASAN 31](#_Toc178103670)

[4.1. *Plan* (Perencanaan) 31](#_Toc178103671)

[4.1.1. Kebutuhan Fungsional 32](#_Toc178103672)

[4.1.2. Kebutuhan Non-Fungsional 33](#_Toc178103673)

[4.2. *Design* (Desain) 33](#_Toc178103674)

[4.2.1. Arsitektur Sistem 33](#_Toc178103675)

[4.2.2. *Class Diagram* 35](#_Toc178103676)

[4.2.3. *Use Case Diagram* 36](#_Toc178103677)

[4.2.4. *Sequence Diagram* 37](#_Toc178103678)

[4.2.5. *Data Flow Diagram* 38](#_Toc178103679)

[4.3. *Development* (Pengembangan) 39](#_Toc178103680)

[4.3.1. *Smart Contract* 39](#_Toc178103681)

[4.3.2. Pengembangan Antarmuka 41](#_Toc178103682)

[4.4. *Testing* (Pengujian) 44](#_Toc178103683)

[4.4.1. Pengujian *Smart Contract* 44](#_Toc178103684)

[4.4.2. *Mock Election* 46](#_Toc178103685)

[BAB V SIMPULAN DAN SARAN 54](#_Toc178103686)

[4.3. Kesimpulan 54](#_Toc178103687)

[4.3. Saran 54](#_Toc178103688)

[DAFTAR PUSTAKA 62](#_Toc178103689)

DAFTAR GAMBAR

[Gambar 1.1. Kerangka Pemikiran Penelitian 13](#_heading=)

[Gambar 2.1. Struktur Blok dalam sebuah *Blockchain* 23](#_heading=)

[Gambar 2.2. Struktur *Smart Contract* 26](#_heading=)

[Gambar 3.1. Metode *Agile* 29](#_heading=)

[Gambar 4.1. Arsitektur Sistem 34](#_heading=)

[Gambar 4.2 *Class Diagram* 36](#_heading=)

[Gambar 4.3 *Use Case Diagram* 37](#_heading=)

[Gambar 4.4 *Sequence Diagram* 38](#_heading=)

[Gambar 4.5 *DFD Level 0* 39](#_heading=)

[Gambar 4.6 *DFD Level 1* 39](#_heading=)

[Gambar 4.7 *Smart Contract* 40](#_heading=)

[Gambar 4.8 Rancangan Antarmuka *Home* 41](#_heading=)

[Gambar 4.9 Rancangan Antarmuka *Admin-Login* 42](#_heading=)

[Gambar 4.10 Rancangan Antarmuka *Admin-Dashboard* 42](#_heading=)

[Gambar 4.11 Rancangan Antarmuka *Admin-Candidate* 42](#_heading=)

[Gambar 4.12 Rancangan Antarmuka *Admin-Usermng* 43](#_heading=)

[Gambar 4.13 Rancangan Antarmuka *User-Dashboard* 44](#_heading=)

[Gambar 4.14 Rancangan Antarmuka *User-Vote* 44](#_heading=)

[Gambar 4.15 *Ganache Server Detail* 45](#_heading=)

[Gambar 4.16 Konfigurasi *Metamask* 46](#_heading=)

[Gambar 4.17 *Truffle* *Migrate* 46](#_heading=)

[Gambar 4.18 *Admin-login* 47](#_heading=)

[Gambar 4.19 *Admin-dashboard* 47](#_heading=)

[Gambar 4.20 *Add User* 48](#_heading=)

[Gambar 4.21 *Add Candidate* 48](#_heading=)

[Gambar 4.22 *Add Election* 49](#_heading=)

[Gambar 4.23 *Add Phase* 49](#_heading=)

[Gambar 4.24 *Election* 50](#_heading=)

[Gambar 4.25 *Election-detail* 50](#_heading=)

[Gambar 4.26 *User Identification* 51](#_heading=)

[Gambar 4.27 *Metamask Confirmation* 51](#_heading=)

[Gambar 4.28 *Result* 52](#_heading=)

[Gambar 4.29 *Mining* *Block* 52](#_heading=)

[Gambar 4.30 *Record* *Transaction* 53](#_heading=)

DAFTAR TABEL

[Tabel 2.1 State of the Art 19](#_heading=h.44sinio)

[Tabel 4.1. Kebutuhan Fungsional 32](#_heading=)

[Tabel 4.2. Kebutuhan Non-Fungsional 32](#_heading=)

BAB I PENDAHULUAN

## **1.1. Latar Belakang**

Pemilu merupakan kesempatan bagi masyarakat Indonesia untuk memilih pemimpin dan wakil rakyat pilihannya. Pemilu di Indonesia sendiri masih menggunakan metode tradisional yaitu pemungutan suara di atas kertas dengan mendatangi tempat pemungutan suara yang telah ditentukan pada waktu yang telah ditentukan selama pemilu. Setelah proses pemungutan suara selesai, surat suara dibuka satu per satu dan suara dihitung. Proses tradisional ini memiliki beberapa kelemahan, diantaranya [1]:

1. Besarnya anggaran biaya yang diperlukan untuk tiap pemungutan suara, mulai dari kertas, biaya cetak, gaji untuk panitia dan pengawas, sampai uang transport.
2. Dapat terjadi kecacatan seperti salah cetak, kertas suara robek, data pemilih yang tidak sesuai, hingga data pemilih ganda.
3. Dapat terjadi kecurangan seperti kertas suara yang telah tercoblos,
4. Lambatnya tabulasi hasil perhitungan suara dikarenakan perhitungan dilakukan dengan secara manual, dan keterbatasan infrastruktur.
5. Banyaknya surat suara yang tidak digunakan menimbulkan sampah kertas yang lama kelamaan hal ini akan berdampak pada kelestarian alam.

Karena kompleksitas dan berbagai hambatan dalam pelaksanaannya, proses pemilu tidak berhasil serta kurang efektif dan efisien. Di sisi lain, perkembangan teknologi telah membawa banyak manfaat besar karena menawarkan berbagai kemudahan baik dari segi akses maupun biaya. Penggunaan teknologi informasi dalam penyelenggaraan pemilu akan meningkatkan efektivitas dan efisiensi penerapan transisi ke model pemungutan suara elektronik tradisional. Saat ini, teknologi pemilihan elektronik (*e-voting)* dapat menjadi pilihan yang tepat untuk menyelenggarakan pemilu, salah satu pilar terpenting demokrasi. Selain itu, penerapan metode tradisional yang telah memiliki kelemahan.

Beberapa negara maju dan berkembang juga menerapkan teknologi pemilihan elektronik (*e-voting)*, seperti India, pemilu India adalah sebuah perhelatan demokrasi paling besar di dunia, pada hari pemilu, setiap pemilih harus membawa kartu pemilih, setelah diperiksa oleh panitia pemungutan suara, dan sesuai dengan data daftar pemilih tetap, pemilih diizinkan untuk memilih pada mesin elektronik yang disediakan [2]. Desa Gunungleutik terletak di Kecamatan Ciparay, Kabupaten Bandung, Jawa Barat. Desa ini merupakan salah satu dari beberapa desa yang berada di wilayah Ciparay, dan dikenal sebagai daerah dengan potensi pertanian serta kegiatan masyarakat yang aktif. Dengan total jumlah penduduk 562 jiwa, 287 laki-laki dan 275 perempuan, akan menjadi studi kasus yang cocok untuk penerapan sistem pemilihan elektronik (*e-voting*) berbasis blockchain.

Teknologi *blockchain* dapat mengatasi beberapa masalah kritis dalam sistem pemilihan elektronik, seperti *non-repudiation*, transparansi, dan desentralisasi. Namun, masalah-masalah lain seperti kecepatan transaksi dan perlindungan privasi masih menjadi tantangan utama. Misalnya, skalabilitas blockchain saat ini tidak cukup untuk pemilu nasional karena keterbatasan dalam menangani transaksi dalam jumlah besar[15]. Tujuan dari penelitian ini adalah untuk mengembangkan sistem pemilihan elektronik yang aman, terintegrasi, dan transparan. Penelitian ini akan mencakup perancangan sistem, implementasi sistem, dan evaluasi kinerja sistem pemilihan elektronik berbasis blockchain menggunakan Solidity.

## **1.2. Rumusan Masalah**

Membangun sistem pemilihan elektronik menggunakan *blockchain* ini. Berdasarkan latar belakang yang telah dipaparkan, maka rumusan masalahnya adalah sebagai berikut:

1. Bagaimana mendesain dan mengimplementasikan sistem pemilihan elektronik berbasis *blockchain* menggunakan *solidity*?
2. Bagaimana sistem pemilihan elektronik berbasis *blockchain* dapat mempercepat proses pemilihan dan penghitungan suara, sekaligus mengurangi kesalahan dan risiko kecurangan?
3. Bagaimana pengujian smart contract dalam e-voting dapat memastikan bahwa data pemilih dan hasil suara tidak bisa dimanipulasi atau diakses oleh pihak yang tidak berwenang?

## **1.3. Tujuan Penelitian**

Tujuan dari pembuatan sistem ini adalah sebagai berikut:

1. Merancang dan mengimplementasikan sistem pemilihan elektronik yang aman dan transparan berbasis teknologi *blockchain* menggunakan *solidity* untuk menjamin keamanan dan transparansi data pemilihan.
2. Merancang antarmuka pengguna yang mudah digunakan oleh berbagai kalangan masyarakat, termasuk integrasi dengan dompet digital *MetaMask* untuk autentikasi pemilih.
3. Mengimplementasikan sistem pemilihan elektronik berbasis *blockchain* dalam skenario *mock election* untuk mengukur keefektifan, kemudahan penggunaan, dan tingkat kepercayaan masyarakat terhadap sistem yang dikembangkan.

## **1.4. Manfaat Penelitian**

Berdasarkan tujuan di atas, manfaat penelitian ini dapat dibagi menjadi dua kategori, yaitu manfaat bagi individu (pribadi) dan bagi masyarakat secara umum:

Manfaat bagi pribadi :

1. Peningkatan pengetahuan dan keterampilan. Penelitian ini akan memberikan pengetahuan dan keterampilan baru tentang implementasi teknologi blockchain, terutama dalam sistem pemilihan elektronik. Individu yang mempelajari hasil penelitian ini akan memahami cara kerja blockchain dalam konteks keamanan data dan proses pemilihan yang transparan serta efisien.
2. Pengembangan kompetensi teknologi. Penelitian ini dapat membantu individu yang terlibat dalam pengembangan teknologi informasi, khususnya yang berkaitan dengan keamanan siber, dan sistem terdistribusi untuk mengembangkan kompetensi dalam penerapan teknologi *blockchain* pada sistem yang lebih kompleks seperti pemilu.

Manfaat bagi Masyarakat:

1. Meningkatkan Kepercayaan terhadap pemilu. Dengan adanya sistem pemilihan elektronik berbasis blockchain yang aman, transparan, dan efisien, kepercayaan masyarakat terhadap proses pemilu diharapkan meningkat. Teknologi ini memungkinkan audit yang mudah dilakukan oleh masyarakat luas, sehingga transparansi proses pemilu lebih terjamin.
2. Penyelenggaraan pemilihan menjadi lebih adil dan efisien. *Blockchain* menawarkan sistem yang aman, akurat, anonim, dan adil, yang dapat disesuaikan dengan asas pemilu di Indonesia (langsung, umum, bebas, rahasia, jujur, dan adil). Dengan demikian, masyarakat dapat merasakan manfaat dari proses pemilu yang lebih efisien dan lebih sulit dimanipulasi.

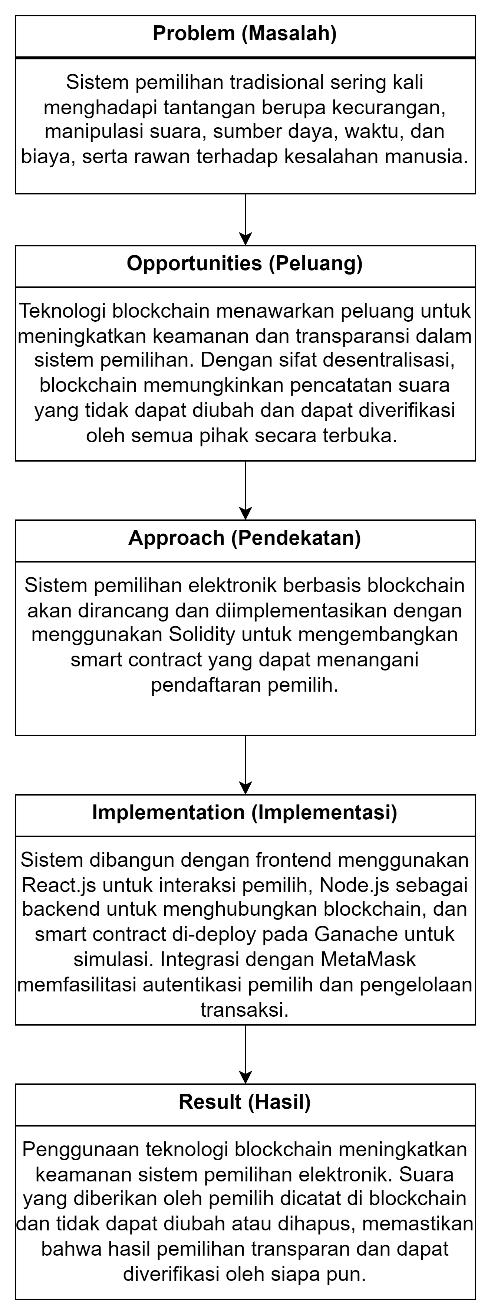
## **1.5. Batasan Masalah**

Penelitian ini mengevaluasi kerangka kerja *blockchain* dan penerapannya sebagai layanan untuk sistem pemilihan elektronik sehingga penelitian yang dilakukan akan dibatasi menjadi berikut ini:

1. Penelitian ini terbatas pada penggunaan teknologi *blockchain Ethereum* dan bahasa pemrograman *Solidity* untuk merancang dan mengimplementasikan sistem pemilihan elektronik.
2. Sistem yang dikembangkan akan memungkinkan pemilih untuk memberikan suara mereka secara elektronik, menyimpan dan mencatat suara secara aman di dalam *blockchain*.
3. Penelitian ini akan memperhatikan skala yang cocok untuk implementasi pemilihan elektronik berbasis *blockchain*. Namun, skala ekstensif atau implementasi pada tingkat nasional tidak akan menjadi fokus pada tahap ini, penelitian ini akan fokus pada skala pemilihan kepala desa, yaitu di desa Gunungleutik, Kecamatan Ciparay.
4. Penelitian ini akan menggunakan simulasi dengan menggunakan *data dummy*.

## **1.6. Kerangka Pemikiran Penelitian**

Pada Gambar 1.1 merupakan kerangka pemikiran yang digunakan dalam penelitian ini:



#### Gambar 1.1. Kerangka Pemikiran Penelitian

## **1.7. Sistematika Penulisan**

Penelitian ini disusun dengan sistematika penulisan yang bertujuan untuk memberikan gambaran umum. Sistematika penulisan pada tugas akhir ini adalah sebagai berikut:

**BAB I: Pendahuluan**

Bab ini menguraikan pendahuluan penelitian, yang meliputi latar belakang penelitian, rumusan masalah, tujuan penelitian, batasan masalah, kerangka pemikiran, dan sistematika penulisan.

**BAB II: Kajian Literatur**

Bab ini membahas kajian literatur yang meliputi tinjauan terhadap penelitian-penelitian sebelumnya serta penjelasan mengenai sejumlah teori yang relevan untuk mengatasi permasalahan penelitian.

**BAB III: Metodologi Penelitian**

Bab ini membahas metode penelitian yang diimplementasikan dalam kajian ini, disertai dengan penjelasan terperinci mengenai setiap langkah dan teknik yang digunakan dalam penelitian.

**BAB IV: Hasil dan Pembahasan**

Bab ini menguraikan tentang proses dan hasil yang telah diperoleh dalam penelitian ini.

**BAB V: Simpulan dan Saran**

Bab ini menjelaskan tentang bagian akhir dari penelitian, seperti kesimpulan secara keseluruhan yang dapat menjawab rumusan masalah dengan saran untuk penelitian selanjutnya dan bertujuan untuk mengembangkan penelitian lebih lanjut.

BAB II KAJIAN LITERATUR

## **2.1. *State of the Art***

Penelitian ini menggali informasi dari beberapa penelitian sebelumnya sebagai bahan perbandingan, baik mengenai kekurangan maupun kelebihan yang sudah ada. Selain itu, informasi juga diperoleh dari buku-buku, jurnal ilmiah, dan skripsi untuk mendapatkan pemahaman tentang teori-teori yang relevan dengan topik penelitian, sehingga dapat membangun landasan teori ilmiah yang kuat. Sistem Pemilihan Elektronik sebelumnya sudah pernah dibuat dan digunakan, namun dalam program aplikasi yang berbeda-beda. Beberapa sistem Pemilihan Elektronik yang berhubungan dengan yang pernah dibuat adalah :

* + 1. Kevin Curran [14] membuat sebuah penelitian yang berjudul "*E-Voting on the Blockchain*", membahas potensi penggunaan teknologi *blockchain* untuk sistem pemungutan suara elektronik yang aman dan andal. penelitian ini menyoroti tantangan dalam membangun sistem pemungutan suara elektronik yang aman dan mengutip sistem pemungutan suara online yang ditinggalkan oleh Pentagon, Amerika Serikat sebagai contoh. Penelitian ini mengeksplorasi penggunaan teknologi *blockchain* untuk mengatasi tantangan-tantangan ini, dengan fokus pada potensinya untuk pemungutan suara yang aman, dapat diandalkan, dan *anonim*. Membangun sebuah sistem pemungutan suara elektronik yang aman itu sulit, seperti yang ditunjukkan oleh sistem pemungutan suara online yang ditinggalkan oleh Pentagon AS. Teknologi blockchain berpotensi untuk menjawab tantangan keamanan dan keandalan dalam sistem pemungutan suara elektronik. Penelitian ini membahas berbagai penelitian dan implementasi sistem pemungutan suara elektronik berbasis *blockchain*, seperti *Bitcoin*, *Ethereum*, *Hyperledger Fabric*, dan *Hyperledger Sawtooth*. Penelitian ini juga membahas masalah yang berkaitan dengan skalabilitas, privasi, dan keamanan dalam sistem pemungutan suara elektronik berbasis blockchain.
    2. Uzma Jafar, Mohd Juzaiddin Ab Aziz, dan Zarina Shukur [15] dengan penelitian yang berjudul "*Blockchain for Electronic Voting System—Review and Open Research Challenges*" memberikan tinjauan yang komprehensif mengenai penggunaan teknologi *blockchain* pada sistem pemungutan suara elektronik. Penelitian ini mendiskusikan manfaat potensial dari sistem *e-voting* berbasis *blockchain*, seperti keamanan, integritas, dan transparansi, serta tantangan yang perlu diatasi untuk implementasi yang sukses. Pemungutan suara online semakin populer karena potensinya untuk mengurangi biaya penyelenggaraan dan meningkatkan jumlah pemilih. Teknologi *blockchain* dapat meningkatkan keamanan dan integritas sistem pemungutan suara elektronik. Penelitian ini membahas berbagai penelitian dan implementasi sistem *e-voting* berbasis *blockchain*, seperti *DecentraVote*, Sistem *E-Voting* Berbasis *Blockchain*, dan *framework* Int & Inter. Penelitian ini menyoroti manfaat dari sistem *e-voting* berbasis *blockchain*, termasuk keamanan, integritas, dan transparansi. Penelitian ini juga membahas tantangan yang dihadapi dalam mengimplementasikan sistem *e-voting* berbasis *blockchain*, seperti skalabilitas, privasi, dan kecepatan transaksi. Penelitian ini menyimpulkan bahwa meskipun teknologi *blockchain* menjanjikan sistem pemungutan suara elektronik yang aman dan dapat diandalkan, masih ada tantangan yang harus dihadapi, seperti perlindungan privasi, skalabilitas, dan kecepatan transaksi. Mereka menyarankan bahwa penelitian lebih lanjut diperlukan untuk mengatasi tantangan-tantangan ini dan sepenuhnya menyadari potensi sistem *e-voting* berbasis *blockchain*.
    3. Basit Shahzad dan Jon Crowcroft [16] dengan penelitian yang berjudul "*Trustworthy Electronic Voting Using Adjusted Blockchain Technology*" membahas keefektifan penggunaan teknologi *blockchain* untuk meningkatkan keamanan dan integritas sistem pemungutan suara elektronik. Penelitian ini mengusulkan sebuah *framework* yang menjawab tantangan sistem *e-voting* berbasis *blockchain*, seperti skalabilitas, privasi, dan kecepatan transaksi. Penelitian ini mendiskusikan tantangan dalam membangun sebuah sistem pemungutan suara elektronik yang aman dan mengutip sistem pemungutan suara online yang ditinggalkan oleh Pentagon Amerika Serikat sebagai contoh. *Framework* yang diusulkan berfokus pada keefektifan proses pemungutan suara, algoritma *hashing*, pembuatan dan penyegelan blok, akumulasi data, dan banyak lagi. Penelitian ini menyoroti manfaat dari sistem *e-voting* berbasis *blockchain*, termasuk keamanan, integritas, dan transparansi. Penelitian ini juga membahas tantangan yang dihadapi dalam mengimplementasikan sistem *e-voting* berbasis *blockchain*, seperti skalabilitas, privasi, dan kecepatan transaksi. Penelitian ini menyimpulkan bahwa meskipun teknologi *blockchain* menjanjikan sistem pemungutan suara elektronik yang aman dan dapat diandalkan, masih ada tantangan yang harus diatasi, seperti perlindungan privasi, skalabilitas, dan kecepatan transaksi. Penelitian ini menyarankan bahwa penelitian lebih lanjut diperlukan untuk mengatasi tantangan-tantangan ini dan sepenuhnya menyadari potensi sistem *e-voting* berbasis *blockchain*. Penelitian ini berkontribusi pada penelitian yang sedang berlangsung di bidang sistem *e-voting* berbasis *blockchain* dan memberikan implementasi praktis dari teknologi untuk pemilihan elektronik.
    4. Setiawan Restu Aji, Wahyuningdiah Trisari Harsanti Putri [17] "Implementasi Teknologi *Blockchain* dalam Aplikasi *E-Voting* Berbasis *Mobile*" oleh membahas tentang implementasi teknologi *blockchain* dalam sistem pemungutan suara elektronik berbasis *mobile*. Penelitian ini berfokus pada penggunaan *blockchain* untuk mengatasi masalah keamanan dan integritas pada aplikasi *e-voting* dan pengembangan aplikasi *e-voting* berbasis *mobile* untuk meningkatkan aksesibilitas. Penelitian ini mendiskusikan tantangan dalam membangun sistem pemungutan suara elektronik yang aman. Solusi yang diusulkan berfokus pada penggunaan teknologi blockchain untuk meningkatkan keamanan dan integritas sistem pemungutan suara elektronik. Penelitian ini menyoroti manfaat dari sistem e-voting berbasis blockchain, termasuk keamanan, integritas, dan transparansi. Penelitian ini membahas tantangan yang dihadapi dalam mengimplementasikan sistem e-voting berbasis blockchain, seperti skalabilitas, privasi, dan kecepatan transaksi.
    5. Fadli Fajri, Singgih Jatmiko, dan Missa Lamsani [18] “*Electronic Voting Using Decentralized System Based on Ethereum Blockchain*” merupakan penelitian yang mengeksplorasi implementasi sistem pemungutan suara elektronik yang terdesentralisasi dengan menggunakan teknologi *blockchain* *ethereum*. Penelitian ini bertujuan untuk menjawab tantangan sistem pemungutan suara elektronik tradisional, seperti keamanan, integritas, dan ketergantungan pada otoritas pusat. Penelitian ini mengusulkan sebuah sistem terdesentralisasi yang menggunakan blockchain Ethereum untuk memastikan keamanan, integritas, dan transparansi dalam proses pemungutan suara. Sistem ini dirancang untuk dapat diakses melalui perangkat seluler, yang meningkatkan partisipasi dan aksesibilitas pemilih. Penelitian ini menyoroti manfaat penggunaan teknologi blockchain untuk mengatasi masalah keamanan dan integritas dalam sistem pemungutan suara elektronik. Penelitian ini juga membahas pengembangan aplikasi *e-voting* berbasis seluler untuk meningkatkan aksesibilitas dan kontribusi penelitian terhadap pengembangan aplikasi blockchain dalam berbagai konteks pemilu.
    6. Hjálmarsson dan Gunnlaugur K. Hreiðarsson [16] "*Blockchain-Based E-Voting System*" Tujuan dari penelitian ini adalah mengevaluasi penggunaan teknologi blockchain untuk membangun sistem e-voting yang aman dan terdistribusi. Penelitian ini mengidentifikasi batasan teknologi dan hukum terkait penggunaan blockchain dan mengusulkan sistem baru yang dapat mengatasi batasan tersebut. Tujuan ini jelas dan sesuai dengan isu keamanan pemilu yang sering menjadi perhatian dalam demokrasi modern. Penelitian ini menggunakan metode evaluasi terhadap beberapa framework blockchain populer seperti Exonum, Quorum, dan Geth. kemudian penelitian mengusulkan sistem yang menggunakan blockchain "*permissioned*" berbasis konsensus *Proof of Authority* (PoA) yang dirancang untuk memenuhi persyaratan pemilu. Penelitian ini juga menunjukkan bahwa sistem blockchain dapat memperbaiki keamanan pemilu dan mengurangi biaya operasional. Misalnya, penggunaan kontrak pintar dalam sistem mereka memungkinkan perhitungan suara yang lebih cepat dan terverifikasi secara otomatis oleh beberapa node. Penelitian ini menyimpulkan bahwa teknologi blockchain menawarkan potensi besar untuk pemilu demokratis yang lebih aman, transparan, dan hemat biaya. Namun, sistem ini masih memerlukan pengembangan lebih lanjut dalam hal skalabilitas dan ketahanan terhadap serangan.
    7. Zheng, Zibin, Xie, Shaoan, Dai, dan Hong-Ning. Dalam penelitianya yang berjudul “*Blockchain challenges and opportunities*: *A survey*” [8]. Penelitian ini membahas tentang teknologi blockchain, yang memiliki banyak kelebihan seperti decentralisasi, persistensi, anonimitas, dan auditabilitas. Meskipun banyak penelitian yang memfokuskan pada penggunaan teknologi blockchain dalam berbagai aspek aplikasi, belum ada survei yang komprehensif tentang teknologi *blockchain* dari perspektif teknis dan aplikatif. Penelitian ini menjelaskan bahwa blockchain dapat dianggap sebagai buku besar publik, di mana semua transaksi yang dikomitmen disimpan dalam rantai blok yang terus tumbuh ketika blok baru ditambahkan. diakhiri dengan membahas arah masa depan teknologi *blockchain*, termasuk kebutuhan untuk mengembangkan algoritma konsensus yang lebih efisien dan solusi untuk menangani tantangan yang diidentifikasi.
    8. Wu, K., Liu, M., & Xu, J. Pada penelitianya yang berjudul “*How Will Blockchain Technology Impact Auditing and Accounting: Permissionless Vs. Permissioned Blockchain”* [4]. Menjelajahi dampak potensial teknologi blockchain terhadap praktik audit dan akuntansi. Penelitian ini membedah perbedaan antara *permissionless blockchain* dan *permissioned blockchain*, serta mengulas bagaimana variasi ini mungkin mempengaruhi proses audit dan akuntansi. *Permissionless blockchain* terbuka untuk siapa saja dan tidak memerlukan izin sebelumnya untuk berpartisipasi. Contoh termasuk *Bitcoin* dan *Ethereum*. Penelitian ini membahas tantangan yang terkait masalah skalabilitas dan potensi aktivitas berbahaya. Sedangkan *permissioned blockchain* dikontrol oleh kelompok tertentu atau organisasi dan memerlukan izin untuk bergabung ke jaringan.
    9. Mohanta, Bhabendu & Panda, Soumyashree & Jena, Debasish. Dalam penelitianya yang berjudul “*An Overview of Smart Contract and Use Cases in Blockchain Technology”* [23]. Memberikan gambaran menyeluruh tentang *smart contract* dan aplikasinya dalam teknologi *blockchain*. Penelitian ini menjelaskan konsep dasar dari *smart contract*, cara kerjanya, serta berbagai kasus penggunaan yang relevan dalam berbagai industri. Penelitian ini menjelaskan bahwa *smart contract* adalah program komputer yang secara otomatis mengeksekusi, mengontrol, atau mendokumentasikan peristiwa dan tindakan sesuai dengan ketentuan kontrak. Kontrak ini disimpan di dalam *blockchain* dan dapat dieksekusi tanpa memerlukan pihak ketiga. Penelitian ini mengurai beberapa karakteristik dari *smart contract* yaitu otomatisasi, transparansi dan keamanan, dengan beberapa pengguanaan seperti pada sektor keungan, kesehatan dan pendidikan. Dengan menjelaskan karakteristik utama, kasus penggunaan yang relevan, serta tantangan yang dihadapi, penelitian ini menjadi sumber informasi yang berharga bagi peneliti, pengembang, dan profesional di bidang teknologi informasi yang tertarik pada inovasi *blockchain*.
    10. Salman, S. A. B., Al-Janabi, S., & Sagheer, A. M. [27]. Dalam penelitianya yang berjudul “*A Review on E-Voting Based on Blockchain Models*.” memberikan gambaran menyeluruh tentang penggunaan *blockchain* dalam sistem *e-voting*. Penelitian ini menjelaskan apakah *blockchain* dapat digunakan untuk membangun sistem *e-voting* yang efisien, serta mengidentifikasi beberapa teknologi *blockchain* yang relevan dan kelebihan serta kekurangannya. Sistem *e-voting* adalah cara modern untuk melakukan pemungutan suara secara *online* menggunakan kriptografi. Pemungutan suara dapat dilakukan dari kenyamanan rumah menggunakan komputer atau perangkat *mobile*. Hasil pemungutan suara akhir dapat dihitung secara otomatis oleh *server* pusat. Kesulitan dalam sistem e-voting meliputi integritas data, keandalan, privasi suara, konsekuensi gangguan, pemungut suara yang tidak terdidik, keterampilan IT yang spesialis, penyimpanan peralatan, keamanan, efek penipuan, dan biaya. Dalam beberapa tahun terakhir, penggunaan *blockchain* dalam sistem *e-voting* telah menjadi pilihan yang lebih penting untuk mengatasi banyak masalah keamanan yang mungkin timbul dengan sistem *e-voting*. *Blockchain* memungkinkan pemerintah untuk mengimplementasikan sistem pemungutan suara cerdas yang terintegrasi dengan informasi keberlanjutan untuk memastikan bahwa semua anggota memiliki informasi yang akurat tentang properti yang sedang berlangsung. Penelitian ini menyimpulkan dengan membahas potensi masa depan dari penggunaan *blockchain* dalam sistem *e-voting*. Mereka menekankan bahwa seiring dengan kemajuan teknologi *blockchain* dan peningkatan pemahaman tentang penggunaannya, blockchain akan semakin banyak diterapkan di berbagai industri untuk meningkatkan keamanan, transparansi, dan efisiensi dalam pemungutan suara.

Secara umum, penelitian sebelumnya lebih berfokus pada tantangan penelitian terbuka dan peluang masa depan dalam *blockchain* untuk *e-voting*, sedangkan penelitian perancangan dan implementasi sistem elektronik berbasis blockchain menggunakan solidity menawarkan solusi implementasi teknis langsung dalam bentuk kontrak pintar untuk e-voting. Penelitian sebelumnya menekankan kebutuhan akan inovasi dalam hal privasi dan skalabilitas, sementara penelitian ini menunjukkan bagaimana teknologi ini bisa diimplementasikan secara nyata dalam sistem pemilu meskipun masih terbatas dalam skala besar. Kebaruan dari penelitian ini terletak pada desain sistem nyata yang menggunakan *solidity* untuk mengembangkan sistem *e-voting* yang dapat diuji dan digunakan. Penelitian ini menunjukkan bagaimana *smart contract* dapat menggantikan peran otoritas pemilihan dalam menghitung suara dan menjaga transparansi, memberikan solusi langsung dan praktis untuk beberapa tantangan yang disebutkan dalam penelitian sebelumnya seperti transparansi dan otomasi proses. Penelitian ini memberikan kontribusi baru dengan mengusulkan penggunaan *blockchain* *permissioned* berbasis *PoA* untuk sistem *e-voting* dan mengeksplorasi aplikasi *smart contract* untuk pemilu. Selain itu, integrasi *face recognition* untuk menjaga privasi suara menunjukkan pendekatan inovatif terhadap masalah privasi dalam pemilu.

##### Tabel 2.1 *State of the Art*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Judul** | **Penulis** | **Tahun** | **Pembahasan** |
| 1 | *E-Voting on the Blockchain* | Kevin Curran | 2018 | Penelitian ini mengeksplorasi penggunaan teknologi *blockchain* untuk mengatasi tantangan-tantangan ini, dengan fokus pada potensinya untuk pemungutan suara yang aman, dapat diandalkan, dan *anonim*. |
| 2 | *Blockchain for Electronic Voting System—Review and Open Research Challenges* | Uzma Jafar, Mohd Juzaiddin Ab Aziz, dan Zarina Shukur | 2021 | Penelitian ini mendiskusikan manfaat potensial dari sistem *e-voting* berbasis *blockchain*, seperti keamanan, integritas, dan transparansi, serta tantangan yang perlu diatasi untuk implementasi yang sukses. |
| 3 | *Trustworthy Electronic Voting Using Adjusted Blockchain Technology* | Basit Shahzad dan Jon Crowcroft | 2019 | Penelitian ini membahas keefektifan penggunaan teknologi *blockchain* untuk meningkatkan keamanan dan integritas sistem pemungutan suara elektronik. Penelitian ini mengusulkan sebuah *framework* yang menjawab tantangan sistem *e-voting* berbasis *blockchain*, seperti skalabilitas, privasi, dan kecepatan transaksi. |
| 4 | Implementasi Teknologi *Blockchain* dalam Aplikasi *E-Voting* Berbasis *Mobile* | Setiawan Restu Aji, Wahyuningdiah Trisari Harsanti Putri | 2023 | Penelitian ini membahas tentang implementasi teknologi *blockchain* dalam sistem pemungutan suara elektronik berbasis *mobile*. Penelitian ini berfokus pada penggunaan *blockchain* untuk mengatasi masalah keamanan dan integritas pada aplikasi *e-voting* dan pengembangan aplikasi *e-voting* berbasis *mobile* untuk meningkatkan aksesibilitas. |
| 5 | *Electronic Voting Using Decentralized System Based on Ethereum Blockchain* | Fadli Fajri, Singgih Jatmiko, dan Missa Lamsani | 2020 | Penelitian ini mengusulkan sebuah sistem terdesentralisasi yang menggunakan blockchain Ethereum untuk memastikan keamanan, integritas, dan transparansi dalam proses pemungutan suara. |
| 6 | *Blockchain-Based E-Voting System* | Hjálmarsson dan Gunnlaugur K. Hreiðarsson | 2018 | Teknologi blockchain menawarkan potensi besar untuk pemilu demokratis yang lebih aman, transparan, dan hemat biaya. Namun, sistem ini masih memerlukan pengembangan lebih lanjut dalam hal skalabilitas dan ketahanan terhadap serangan. |
| 7 | *Blockchain challenges and opportunities*: *A survey* | Zheng, Z., Xie, S., Dai, H-N., Chen, X., & Wang, H. | 2018 | Membahas tentang teknologi blockchain, yang memiliki banyak kelebihan seperti decentralisasi, persistensi, anonimitas, dan auditabilitas. |
| 8 | *How Will Blockchain Technology Impact Auditing and Accounting: Permissionless Vs. Permissioned Blockchain* | Wu, K., Liu, M., & Xu, J. | 2019 | Menjelajahi dampak potensial teknologi blockchain terhadap praktik audit dan akuntansi. Penelitian ini membedah perbedaan antara *permissionless blockchain* dan *permissioned blockchain*, serta mengulas bagaimana variasi ini mungkin mempengaruhi proses audit dan akuntansi. |
| 9 | *An Overview of Smart Contract and Use Cases in Blockchain Technology* | Mohanta, Bhabendu & Panda, Soumyashree & Jena, Debasish | 2018 | Memberikan gambaran menyeluruh tentang *smart contract* dan aplikasinya dalam teknologi *blockchain*. Penelitian ini menjelaskan konsep dasar dari *smart contract*, cara kerjanya, serta berbagai kasus penggunaan yang relevan dalam berbagai industri. |
| 10 | *A Review on E-Voting Based on Blockchain Models.* | Salman, S. A. B., Al-Janabi, S., & Sagheer, A. M. | 2022 | Penelitian ini menjelaskan apakah *blockchain* dapat digunakan untuk membangun sistem *e-voting* yang efisien, serta mengidentifikasi beberapa teknologi *blockchain* yang relevan dan kelebihan serta kekurangannya. |

## **2.2. Dasar Teori**

Dasar teori adalah landasan atau struktur konseptual yang dipergunakan untuk menguraikan teori-teori yang relevan dalam mendukung suatu penelitian. Berikut adalah dasar teori yang bisa mendukung penelitian ini:

### **2.2.1. Blockchain**

*Blockchain* adalah teknologi revolusioner yang memberikan dampak besar pada masyarakat modern karena transparansi, desentralisasi, dan keamanannya. *Blockchain* mendapatkan perhatian yang cukup besar karena aplikasi pertama dari mata uang digital, misalnya *Bitcoin*. Dalam waktu dekat, teknologi *Blockchain* bertekad untuk mengubah cara kita hidup, berinteraksi, dan menjalankan bisnis. Baru-baru ini, para akademisi, industrialis, dan peneliti secara agresif menyelidiki berbagai aspek *Blockchain* sebagai teknologi yang sedang berkembang [7], tidak hanya transfer uang tetapi juga semua jenis informasi struktural dapat disimpan dalam *blockchain* ini, dan dengan bantuan beberapa metode *kriptografi*, sistem dapat dipertahankan dengan aman [3]. Banyak informasi dapat direkam dengan sistem ini dengan modifikasi yang relevan. *ethereum* misalnya, *cryptocurrency* lain dengan lingkungan pengembangan multiguna, yang muncul beberapa tahun setelah *bitcoin*, membedakan *blockchain* secara nyata, mengungkapkan bahwa teknologi ini dapat menghasilkan perangkat lunak yang dapat menyimpan informasi yang terstruktur seperti dijelaskan di atas. Selain itu, ada manfaat yang dimiliki *blockchain* yang dapat digunakan dalam mendesain sistem yaitu [4]:

1. *Security*, Dengan menggunakan enkripsi asimetris. Kunci yang dihasilkan adalah dalam bentuk dua pasang kunci publik dan privat yang terkait secara matematis. Kunci publik akan dipublikasikan dalam sistem dan kunci pribadi hanya diakses oleh pengguna. Hanya orang yang memiliki kunci pribadi yang dapat menggunakan akun.
2. *Accuracy*, Dalam pemilihan setiap pengguna akan diverifikasi oleh lembaga dan mendaftar sehingga pengguna yang dapat memilih adalah pengguna yang sudah diverifikasi
3. *Transparency*, Semua surat suara dalam sistem disimpan di *blockchain* sehingga pengguna dapat melihat berapa banyak suara yang dimiliki masing masing kandidat, selain itu sistem ini dapat dan mudah diaudit.
4. *Autonomy*, Hal besar yang mengikuti sistem pemungutan suara ini adalah bahwa memiliki keuntungan di bidang sistem desentralisasi.
5. *Anonymity*, Sistem pemungutan suara yang digunakan adalah anonim dimana penyimpanan data yang terdapat di dalam *blockchain* tidak ada data mengenai pemilih melainkan hanya berupa alamat publik dari setiap dompet digital karena dalam *blockchain* itu sendiri hanya mencatat
6. *Fairness*, setiap pengguna dapat memilih sesuai pilihan mereka.
7. *Efficiency*, Target yang diharapkan dari sistem ini adalah untuk meminimalkan biaya yang digunakan untuk operasi.

*Blockchain* merupakan sebuah buku besar yang dapat diakses oleh publik dan setiap transaksi yang terjadi dicatat dalam blok yang saling terhubung satu dengan yang lainnya sehingga berbentuk seperti rantai [8]. *Blockchain* juga bisa disebut sebuah basis data terdistribusi dari catatan atau buku besar dari semua transaksi yang telah dieksekusi dan dibagikan kepada pihak-pihak yang berpartisipasi. Setiap transaksi dalam buku besar diverifikasi oleh konsensus mayoritas peserta dalam sistem. Dan sekali masuk, informasi tidak akan pernah bisa dihapus. Dalam teknologi blockchain, blockchain dapat dibagi menjadi 3 jenis yaitu [8]:

1. *Public Blockchain,* merupakan jaringan yang terdistribusi secara besar serta dapat diakses bagi siapa saja untuk berpartisipasi dan memiliki kode *open source* yang dikelola oleh komunitas pendiri.
2. *Permissioned Blockchain*, adalah jenis *blockchain* yang dapat dijalankan secara individu pada jaringan besar yang terdistribusi tetapi kode intinya ada yang o*pen source* dan tidak.
3. *Private Blockchain*, merupakan tipe *blockchain* yang keanggotaannya dikendalikan secara terpusat atau biasa disebut *Centralized*.

Setiap jenis *blockchain* menggunakan teknologi kriptografi yang memungkinkan setiap anggota di jaringan tertentu untuk mengelola struktur data dengan cara yang aman tanpa perlu otoritas pusat untuk menegakkan aturan. Teknologi Blockchain memiliki cara kerja dengan mendistribusikan buku besar ke dalam jaringan komputer dan melakukan verifikasi. Setiap komputer memiliki buku besar (*Blockchain*) dari semua transaksi yang dicatat untuk diumumkan. Transaksi yang telah melalui verifikasi akan dimasukan ke dalam blok. Selain itu, blok secara permanen akan saling terhubung dengan transaksi yang terjadi sebelum dan sesudahnya dan membentuk sebuah rantai yang dinamakan blockchain. Karena Blockchain terdiri dari dua jenis record, transaksi dan blok. Tidak ada server terpusat untuk transaksi karena setiap blok harus memenuhi syarat dan juga tidak akan menimpa transaksi sebelumnya [9].

Blockchain sendiri terbagi menjadi dua yaitu bitcoin based dan ethereum based dimana ethereum based ini lebih mementingkan keperluan pengembangan blockchainya,

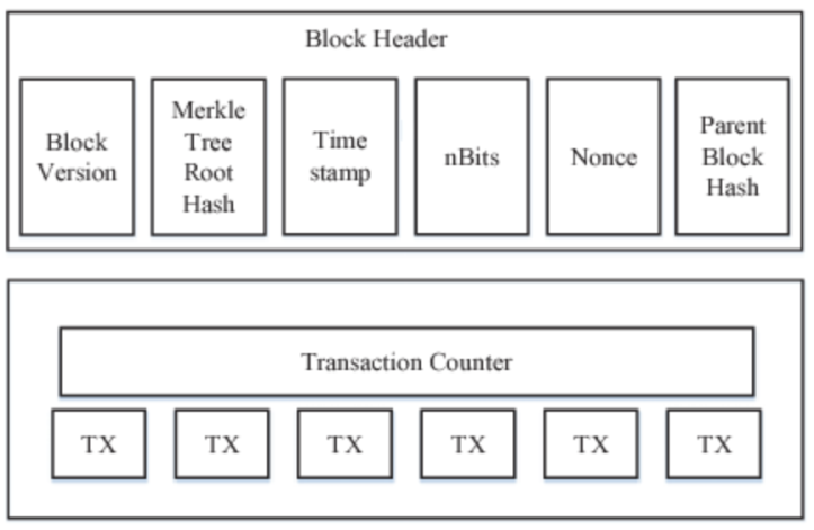
*Blockchain* adalah urutan blok, yang menyimpan daftar lengkap catatan transaksi seperti buku besar publik konvensional. Dalam sebuah blok yang terdapat di blockchain terdapat dua bagian yaitu [8]:

1. *Block header*

Pada block header terdapat:

1. *Block version*, berisikan tentang aturan mana yang harus diikuti.
2. *Merkle Tree Root Hash,* yang berisikan nilai hash dari semua transaksi di blok.
3. *Time Stamp,* yang berisikan waktu saat ini dalam satuan waktu universal.
4. *nBits,* yang berisikan batas dari target blok yang valid.
5. *Nonce,* yang berisikan 4 *byte* yang biasa dimulai dari angka 0 dan meningkat setiap terjadi perhitungan *hash*.
6. *Parent Block Hash,* yang berisikan nilai dari hash sebelumnya.
7. *Block body*

*Block Body* berisikan perhitungan transaksi dan transaksi itu sendiri. Jumlah dari banyaknya transaksi yang dapat ditampung dalam sebuah blok tergantung pada ukurannya.



#### Gambar 2.1. Struktur Blok dalam sebuah *Blockchain* [8]

### **2.2.2. Pemilihan Elektronik**

Pemilihan elektronik, juga dikenal sebagai *e-voting*, adalah proses pemilihan umum atau pemilihan lainnya di mana pemilih menggunakan sistem elektronik, seperti komputer atau perangkat mobile, untuk memberikan suara mereka. Ini berbeda dengan pemilihan tradisional di mana pemilih memberikan suara mereka secara manual dengan menggunakan kertas dan pensil atau alat lainnya. Pemilihan elektronik (*e-voting*) adalah sebuah proses pemungutan suara yang dilakukan dengan bantuan media teknologi informasi yang bertujuan untuk mempercepat dan mempermudah proses pemungutan dan perhitungan suara pada pemilihan umum, serta dapat menggantikan kertas suara [10]. Pemilihan elektronik (*e-voting*) ini pertama kali diperkenalkan oleh *David Shaum* pada awal tahun 1980. Sistem *e-voting* ini menggunakan *cryptography-key* yang dapat membantu para *voter* untuk tetap tidak terdeteksi (*anonym*). *Washington D. C*. pernah mengembangkan pemilihan elektronik pada tahun 2010. Tetapi terjadi banyak sekali masalah keamanan pada saat melakukan pengujian pada sistemnya. Sehingga proyek tersebut gagal untuk diimplementasikan [11].

### **2.2.3. Ethereum**

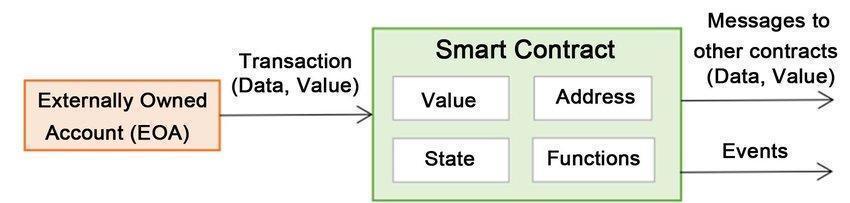
*Ethereum* adalah *platform* perangkat lunak terdesentralisasi yang berjalan di atas teknologi *blockchain*. Diciptakan oleh *Vitalik Buterin* pada tahun 2013 dan diluncurkan pada tahun 2015, *Ethereum* memungkinkan pengembang untuk membangun dan menjalankan aplikasi terdesentralisasi (*DApps*) serta kontrak pintar (*smart contracts*) di atas *blockchain Ethereum*. Dalam beberapa hal, *ethereum* ini tidak berbeda dengan *bitcoin*, tetapi ada beberapa hal yang berbeda diantara keduanya. *Bitcoin* menawarkan sistem *digital currency* yang *peer to peer*, sementara *ethereum* biasanya berfokus untuk penggunaan *smart contract* dari berbagai aplikasi terdesentralisasi [12]. *Ethereum* memberikan kebebasan kepada pengembang untuk membuat program mereka sendiri ke dalam kontrak, sehingga pengembang bebas untuk menerapkan logika bisnis ke dalam *blockchain* (Vujicic et al., 2018). Salah satu keunggulan utama *Ethereum* dibandingkan *blockchain* lainnya adalah dukungan untuk *Turing-complete smart contracts*. Ini memungkinkan pembuatan logika pemrograman yang kompleks, yang sangat penting Sistem Pemilihan Elektronik (*e-voting)* yang membutuhkan berbagai aturan dan kondisi. *Ethereum* memiliki komunitas pengembang yang besar dan ekosistem yang luas. Banyak *tools*, *library*, dan *framework* yang dikembangkan untuk *Ethereum*, membuatnya lebih mudah untuk membangun dan memelihara Sistem Pemilihan Elektronik (*e-voting)*. *Ethereum* ini terus dikembangkan dan ditingkatkan oleh komunitasnya, dengan pembaruan dan peningkatan berkelanjutan. Ini memastikan bahwa jaringan *Ethereum* tetap aman, efisien, dan mampu mengakomodasi kebutuhan aplikasi masa depan.

*Ethereum Virtual Machine* (EVM) adalah jantung dari *ethereum*. Setiap *node* dalam jaringan *ethereum* menjalankan EVM yang dapat mengeksekusi kode algoritma yang kompleks yang ditulis dalam bahasa pemrograman seperti *javascript* dan *python* (P.et al., 2018). Penggunaan *Ethereum* dalam sistem pemilihan elektronik (*e-voting*) didasarkan pada keunggulan teknologi *blockchain* yang menawarkan transparansi, keamanan, dan imutabilitas transaksi. *Smart contract* di *Ethereum* dapat digunakan untuk menjalankan program yang berisi kode yang dieksekusi otomatis ketika kondisi dan persyaratan tertentu terpenuhi. Dalam konteks *e-voting*, *smart contract* dapat mengatur dan mengelola transaksi suara secara otomatis tanpa membutuhkan perantara seperti pengguna hukum atau pihak pengawas. Dengan menggunakan teknologi *Ethereum*, sistem *e-voting* dapat memanfaatkan kontrak pintar (*smart contracts*) untuk memastikan bahwa hanya suara yang sah yang dihitung, suara diberikan secara anonim, dan hasil pemilihan dihitung dengan cepat juga akurat. beberapa keuntungan menggunakan Ethereum dalam Sistem Pemilihan Elektronik:

1. **Transparansi:** Semua transaksi suara dapat dilacak dan diverifikasi di *blockchain*, sehingga memastikan transparansi penuh dalam proses pemilihan.
2. **Keamanan:** *Smart contract* memastikan bahwa data suara tidak dapat diubah setelah dicatat di *blockchain*, sehingga menjamin keamanan dan kejujuran hasil pemilihan.
3. **Imutabilitas:** Data yang dicatat di *blockchain* tidak dapat diubah atau dihapus, menjamin bahwa hasil pemilihan tetap utuh dan bebas dari manipulasi.
4. **Efisiensi:** Dengan menghilangkan perantara dan menjalankan proses pemilihan secara otomatis, *e-voting* berbasis *Ethereum* dapat mengurangi biaya dan meningkatkan efisiensi proses pemilihan.

### **2.2.4. *Smart Contract***

*Smart contract* adalah program yang berjalan di jaringan *blockchain*. *Smart contract* adalah transaksi yang berisi kode yang akan dieksekusi otomatis ketika kondisi dan persyaratan tertentu terpenuhi. *Smart contract* tidak membutuhkan intermediari seperti pengguna hukum atau pihak pengawas untuk menjamin perjanjian. *Smart contract* dapat mengatur dan mengatur transaksi, mengatur proses, dan mengelola aset digital dalam sistem yang tidak tergantung pada pihak tertentu. *Smart contract* yang berjalan di jaringan *blockchain* dapat menjamin transparansi, keamanan, dan imutabilitas dari transaksi. Smart contract dapat digunakan dalam berbagai aplikasi, seperti sistem pemilihan elektronik, sistem keuangan, dan sistem logistik.



#### Gambar 2.2. Struktur *Smart Contract* [23]

*Smart contract* terdiri dari nilai, alamat, status dan fungsi. *Smart contract* membutuhkan sebuah transaksi sebagai *input*, mengeksekusi kode yang sesuai, dan memicu *output*. Sebuah transaksi *Smart contract* dapat dilacak dan tidak dapat diubah. Semua informasi tentang transaksi ada dalam *Smart contract* dilakukan secara otomatis. Karena sistemnya yang dilakukan secara otomatis penggunaan *smart contract* ini dapat menghilangkan pihak ketiga, *smart contract* sendiri dapat digunakan di berbagai bidang seperti [13] :

1. *Supply chain*. Dalam *supply chain*, *smart contract* digunakan untuk membuat sistem menjadi otomatis, aman dan juga transparan.
2. *Internet of Things* (IoT). Penerapan teknologi smart contract pada IoT yaitu untuk membuat sistem menjadi otomatis.
3. *Healthcare system*. Penerapan *smart contract* pada sistem kesehatan yaitu untuk menjaga privasi dari pasien dan juga membuat sistem yang lebih baik dan otomatis serta dengan *smart contract* manusia dapat menulis beberapa syarat dan ketentuan yang dapat diterapkan setelah data dikumpulkan.
4. *Digital right management*. Penerapan *smart contract* dalam manajemen hak cipta yaitu untuk memastikan royalti diterima oleh pembuat karya terkait dengan menggunakan hak kepemilikan dalam teknologi *blockchain*.
5. *Insurance*. Penerapan *smart contract* pada asuransi yaitu untuk membuat sistem yang lebih sederhana dan juga lebih transparan tanpa ada pihak ketiga.
6. *Financial system*. Dengan menggunakan teknologi *smart contract* pada sistem keuangan membuat pengguna dapat mentransfer uang melalui jaringan *peer to peer* tanpa keterlibatan ada pihak ketiga. (Mohanta et al., 2018).

### **2.2.5. *Solidity***

*Solidity* adalah bahasa pemrograman yang digunakan untuk mengembangkan aplikasi berbasis *blockchain*. *Solidity* memungkinkan pengembang untuk mengembangkan aplikasi yang kompatibel dengan Ethereum, yang merupakan platform *blockchain* yang paling populer. *Solidity* adalah *high-level programming language* yang digunakan untuk menulis kontrak pintar (*smart contracts*) di *platform Ethereum*. *Smart contracts* adalah program komputer yang berjalan di atas *blockchain Ethereum* dan dirancang untuk secara otomatis mengeksekusi perjanjian atau kondisi yang telah diprogram saat kondisi tertentu terpenuhi. *Solidity* digunakan untuk mengembangkan *smart contract* yang dapat menyediakan fungsionalitas yang diperlukan untuk aplikasi *blockchain*, seperti menangani transaksi, menyimpan data, dan mengatur kebijakan. *Solidity* memiliki fitur-fitur yang unik, seperti *support* untuk *transient storage* (EIP-1153), *shard blob (binary large object) transactions* (EIP-4844), dan lain-lain[14].

### **2.2.6. *UML (Unified Modeling Language)***

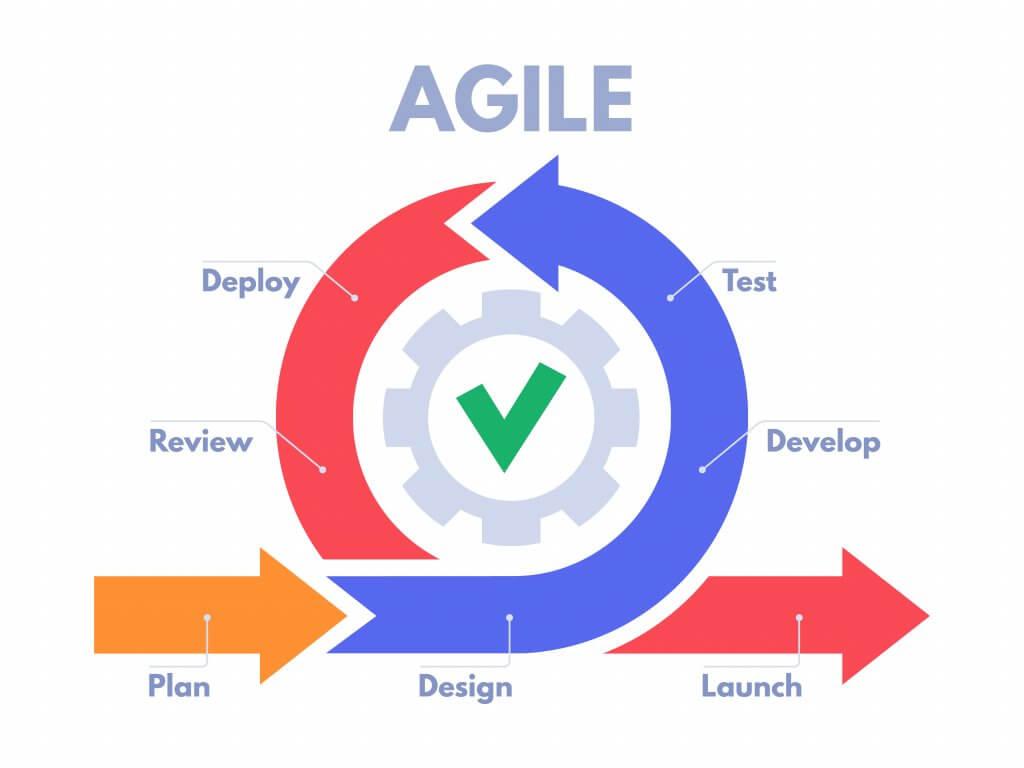
*UML* atau*Unified Modeling Language*, adalah bahasa pemodelan standar yang digunakan untuk menggambarkan, merancang, dan mendokumentasikan sistem perangkat lunak dan non-perangkat lunak. Tujuannya adalah untuk menyediakan notasi yang terstandarisasi sehingga semua pihak yang terlibat dalam pengembangan perangkat lunak termasuk pengembang, analis sistem, dan pemangku kepentingan dapat berkomunikasi dengan lebih efektif. Fungsi dan kegunaan dari UML diantaranya visualisasi, perancangan, dokumentasi dan komunikasi. UML merupakan alat penting dalam pengembangan perangkat lunak modern. Dengan menyediakan notasi standar untuk berbagai aspek desain dan analisis, UML membantu memastikan bahwa semua orang yang terlibat memiliki pemahaman yang sama tentang arsitektur sistem, sehingga meningkatkan efisiensi dan efektivitas proses pengembangan perangkat lunak [25].

### **2.2.6. *Agile***

Metode *Agile* adalah sebuah pendekatan manajemen proyek yang digunakan dalam pengembangan perangkat lunak, yang berfokus pada iterasi, kolaborasi tim, dan fleksibilitas dalam merespon perubahan. Metode *Agile* memecah proyek besar menjadi serangkaian iterasi atau *sprint* yang lebih kecil dan terukur. Setiap sprint biasanya berlangsung selama dua hingga empat minggu. Manfaat yang didapatkan dari sisi developer adalah peningkatan produktivitas. Karena setiap tim dapat mengerjakan setiap tugas tanpa harus menunggu tim lain untuk menyelesaikan tugasnya. Selain itu, developer menjadi memiliki banyak waktu untuk berkembang sesuai dengan keinginan mereka. Dengan demikian, metode Agile merupakan pendekatan manajemen proyek yang efektif dalam pengembangan perangkat lunak, dengan fokus pada iterasi, kolaborasi tim, dan fleksibilitas dalam merespon perubahan [26].

BAB III METODE PENELITIAN

Metode penelitian yang digunakan dalam mengimplementasikan Sistem Pemilihan Elektronik Berbasis Blockchain Menggunakan Solidity yaitu *System Development Life Cycle* (SDLC) yang bertujuan untuk merancang, mengembangkan, dan mengimplementasikan sistem pemilihan elektronik berbasis blockchain. Penelitian ini menggunakan metodologi *Agile* untuk mengembangkan sistem *e-voting* berbasis *blockchain* dengan *Solidity*. Model *Agile* dipilih karena sifatnya yang fleksibel, memungkinkan pengembangan sistem dilakukan dalam beberapa tahapan yang dapat disesuaikan.:



#### Gambar 3.1. Metode *Agile* [26]

## **3.1. *Plan* (Perencanaan)**

Pada tahap ini, langkah-langkah strategis disusun untuk menentukan kebutuhan sistem dan mengidentifikasi fitur-fitur utama. Fokus utama pada tahap perencanaan adalah memahami kebutuhan pengguna, menentukan fitur-fitur utama dari sistem *e-voting* berbasis *blockchain*.

## **3.2. *Design* (Desain)**

Pada tahap desain, arsitektur sistem mulai dirancang secara rinci. Desain meliputi *frontend* yang akan digunakan oleh pemilih, *backend* untuk pengolahan data, serta desain *smart contract* di *blockchain*. Selain itu, alur proses pengguna akan disusun untuk memastikan sistem berjalan lancar dari pendaftaran pemilih hingga penghitungan suara.

## **3.3. *Develop* (Pengembangan)**

Tahap pengembangan adalah implementasi desain ke dalam kode yang dapat dijalankan. Pengembangan dilakukan secara bertahap, dimulai dari fitur paling kritis seperti autentikasi pemilih, pencatatan suara, dan penghitungan hasil.

## **3.4. *Test***

Pengujian dilakukan untuk memastikan bahwa setiap bagian dari sistem berfungsi dengan baik. dua metode pengujian utama akan digunakan: *Smart Contract Testing* dan *Mock Election*.

## **3.5. *Deploy***

Setelah pengujian selesai, sistem akan di-deploy ke lingkungan yang lebih besar, seperti *testnet Ethereum* atau jaringan *blockchain* lokal (seperti *Ganache*) untuk memastikan kelayakannya di skenario nyata.

# **BAB IV**

**HASIL DAN PEMBAHASAN**

## **4.1. *Plan* (Perencanaan)**

Tahap awal untuk memahami tujuan, masalah dan peluang yang perlu dipecahkan, masalah dan peluang yang perlu dipecahkan adalah pada fase perencanaan, Ini melibatkan pengumpulan informasi dari *stakeholder* untuk memahami persyaratan yang diinginkan, seperti keamanan, transparansi, dan efisiensi dalam proses pemilihan. Mengacu pada banyaknya permasalahan dalam pelaksanaan pemilihan tradisional pada latar belakang, maka perlu adanya analisis terhadap sistem pemilihan elektronik yang akan berjalan.

* + - 1. Analisis Berjalan

Dalam pembuatan sistem ini mengacu pada pelaksanaan pemilihan yang sudah ada saat ini terbagi menjadi dua, yaitu pemilihan tradisional dan pemilihan elektronik. Dalam pemilihan tradisional, berbagai masalah seperti kecurangan suara, kurangnya transparansi, dan tingginya biaya operasional masih menjadi tantangan besar. Hal ini berakibat pada rendahnya kepercayaan publik terhadap hasil pemilihan. Sistem manual yang digunakan sulit memastikan bahwa data pemilihan tersebut aman, akurat, transparan, otonom, dan anonim, karena manipulasi suara, *human error*, dan pengawasan yang terbatas.

* + - 1. Analisisi Usulan

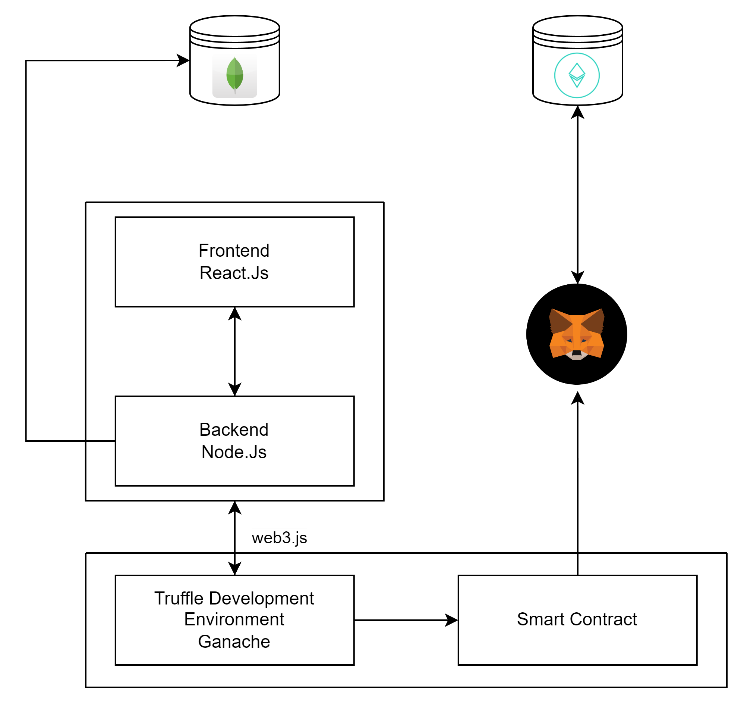
Berdasarkan permasalahan yang diangkat, maka *blockchain* dapat menjadi solusi dalam pembuatan sistem pemilihan elektronik yang dapat membuat sistem pemilihan menjadi lebih aman *blockchain*, dengan sifat desentralisasi dan kriptografi, memberikan jaminan keamanan dan akurasi tinggi dalam mencatat suara. Menurut *Vitalik Buterin*, teknologi *blockchain* memastikan "integritas data yang kuat, karena setiap transaksi atau suara tercatat dalam blok yang tidak dapat diubah setelah dikonfirmasi di jaringan" (*Buterin*, 2017). Dengan demikian, tidak ada aktor tunggal yang bisa memanipulasi hasil pemilihan, memastikan data pemilihan elektronik yang aman dan akurat. transparan, setiap suara yang tercatat di *blockchain* dapat diverifikasi oleh publik, memastikan transparansi penuh.

Dengan pendekatan ini, penggunaan *blockchain* dalam pemilihan elektronik mampu memenuhi tujuan penelitian, yaitu memberikan data pemilihan yang aman, akurat, transparan, otonom, anonim, adil, dan efisien. Pandangan para ahli mendukung implementasi *blockchain* sebagai teknologi yang mampu mengatasi berbagai masalah yang dihadapi dalam pemilihan tradisional, serta meningkatkan kepercayaan publik terhadap sistem pemilihan yang baru.

## **4.2. *Design* (Desain)**

### **4.2.1. Arsitektur Sistem**

Arsitektur Sistem Pemilihan Elektronik Berbasis *Blockchain* menggunakan *Solidity* terdiri dari beberapa lapisan yang saling berinteraksi untuk menyediakan proses pemilihan yang aman dan transparan. Pada lapisan antarmuka pengguna (*frontend*), pemilih dan admin dapat berinteraksi dengan sistem melalui web yang dibangun menggunakan *HTML*, *CSS*, dan *React.js*. Pemilih menggunakan *crypto wallet* seperti *MetaMask* untuk mendaftar, mengautentikasi diri, dan memberikan suara. *Backend*, yang dibangun menggunakan *Node.js*, mengelola logika bisnis dan berkomunikasi dengan *frontend* melalui *middleware*. *Backend* juga berinteraksi dengan *smart contract* di *blockchain* menggunakan *library* *web3.js*. *Smart contract* yang ditulis dalam *Solidity* mengelola pendaftaran pemilih, pemungutan suara, dan penghitungan hasil pemilihan. Semua transaksi dicatat di *blockchain* *Ethereum*, memastikan keamanan dan transparansi. *Database* tradisional dapat digunakan untuk menyimpan data yang tidak sensitif. Berikut adalah arsitektur aplikasi Pemilihan Elektronik Berbasis *Blockchain* menggunakan *Ethereum* menggunakan *Solidity*:

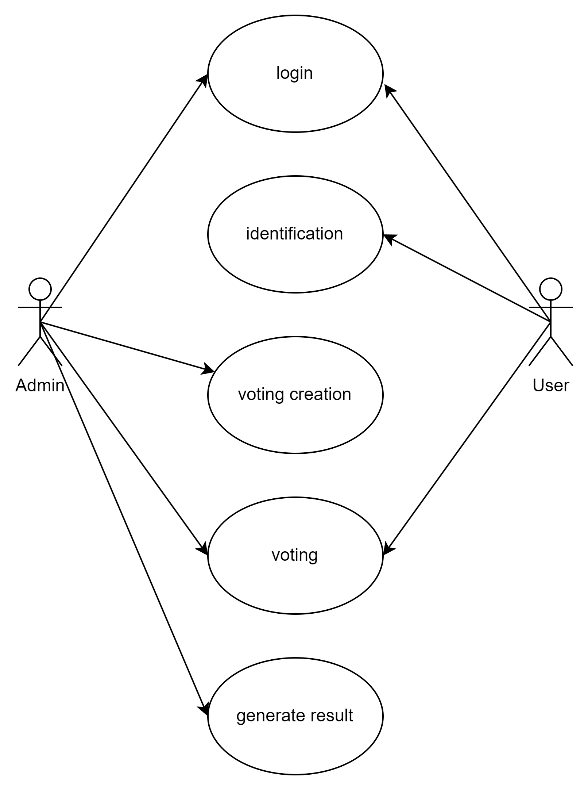


#### Gambar 4.1. Arsitektur Sistem

* + - 1. *Frontend*, menyediakan antarmuka bagi pengguna untuk berinteraksi dengan sistem *e-voting*. *React.js* digunakan sebagai *framework* untuk pengembangan aplikasi web yang dinamis dan cepat, sementara *HTML* dan *CSS* digunakan untuk membangun struktur dan desain visual aplikasi.
      2. *Backend*, *Node.js* digunakan untuk mengelola logika server, termasuk autentikasi pengguna, validasi input, dan interaksi dengan *database.*
      3. *Smart contract*, *Smart contract* yang ditulis dalam *Solidity* bertindak sebagai logika inti untuk *e-voting*, memastikan bahwa semua aturan pemilihan (seperti validasi suara dan pencatatan suara) dijalankan secara otomatis dan transparan di jaringan *blockchain* *ethereum*.
      4. *Ethereum Blockchain*, berfungsi sebagai dasar infrastruktur tempat *smart contract* dieksekusi. Semua transaksi pemilihan, termasuk pendaftaran suara dan pencatatan hasil, dilakukan melalui Ethereum untuk memastikan transparansi dan keamanan.
      5. *Crypto Wallet,* pemilih menggunakan *crypto wallet* seperti *MetaMask* yang memungkinkan pengguna untuk berinteraksi dengan aplikasi berbasis *blockchain* melalui *browser*. Dalam arsitektur ini, *Metamask* digunakan untuk mengelola identitas pengguna, memungkinkan mereka untuk melakukan transaksi dan memberikan suara dalam *e-voting* melalui jaringan *blockchain*.
      6. *MongoDB* digunakan sebagai database *NoSQL* untuk menyimpan data yang tidak sensitif, seperti daftar kandidat, data pengguna (tanpa informasi pribadi yang terkait dengan identitas *blockchain*), dan *metadata* terkait pemilihan.
      7. *Truffle Development Environment, truffle* mempermudah penulisan dan kompilasi *smart contract* yang ditulis dalam *Solidity*. Truffle menangani proses kompilasi kontrak menjadi *bytecode* yang siap di-*deploy* ke *blockchain*. *Truffle* juga digunakan untuk menguji kontrak di *blockchain* lokal, seperti *Ganache*.
      8. *Ganache,* berfungsi sebagai blockchain lokal yang dapat digunakan oleh pengembang untuk melakukan pengujian dan simulasi *smart* *contract* dalam lingkungan yang aman dan terkendali tanpa harus menggunakan jaringan *blockchain* publik.

### **4.2.2. *Use Case Diagram***

*Use case diagram* adalah cara umum untuk mengomunikasikan fungsi-fungsi utama sistem perangkat lunak. Use-case diagram yang paling sederhana adalah representasi interaksi pengguna dengan sistem yang menunjukkan hubungan antara pengguna dan berbagai kasus penggunaan di mana pengguna terlibat. *Use-case diagram* dapat mengidentifikasi berbagai jenis pengguna sistem dan kasus penggunaan yang berbeda dan sering kali disertai dengan jenis diagram lainnya juga. *Use-case diagram* tidak lain adalah fungsi sistem yang ditulis dengan cara yang terorganisir. Hal lain yang relevan dengan use case adalah aktor. Aktor dapat didefinisikan sebagai sesuatu yang berinteraksi dengan sistem.

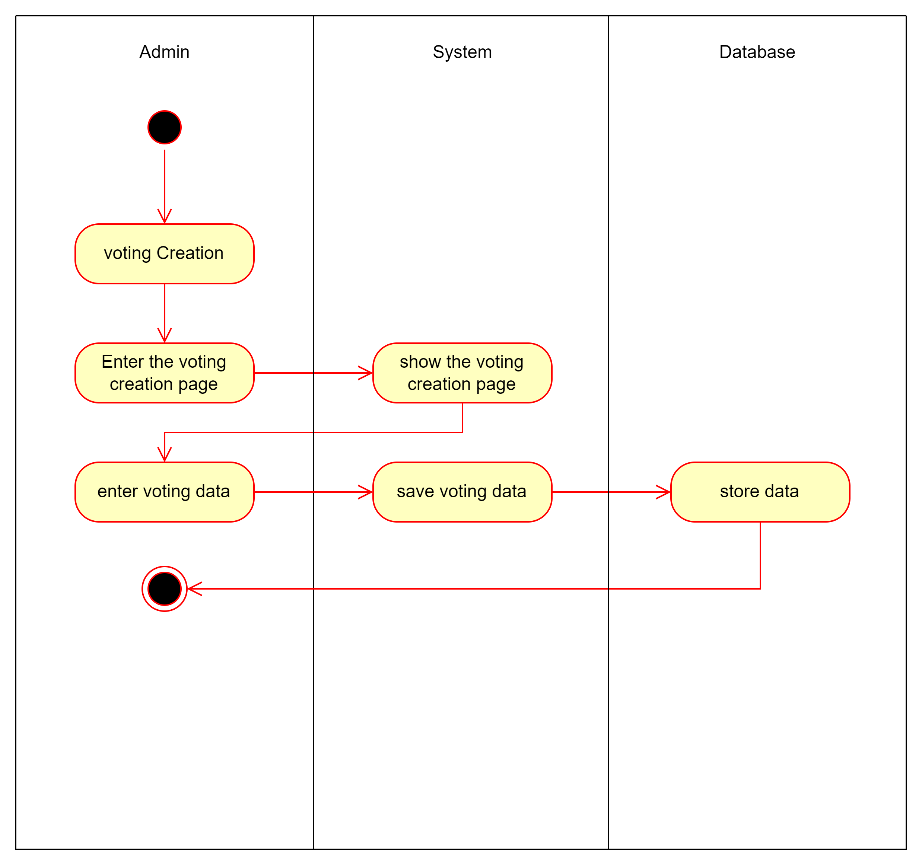


#### Gambar 4.*2 Use Case Diagram*

### **4.2.3. *Activity Diagram***

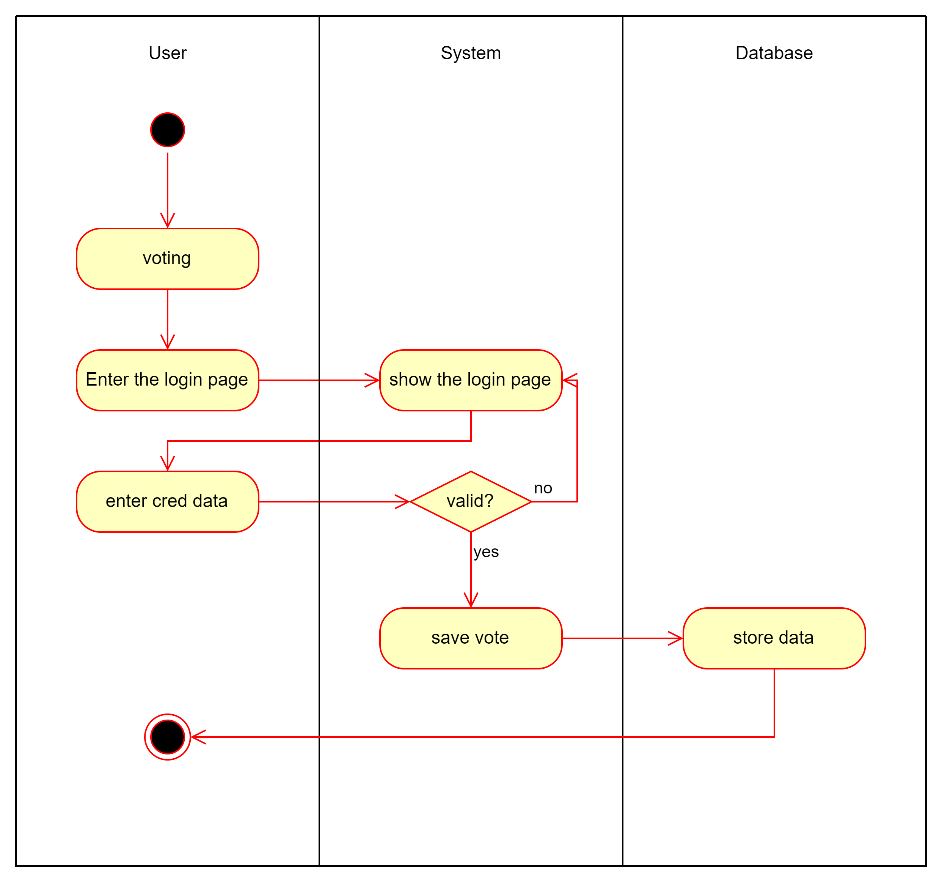
*Activity diagram* adalah salah satu jenis diagram yang digunakan dalam UML untuk memodelkan aliran kerja atau proses bisnis. Diagram ini menggambarkan urutan aktivitas, tindakan, dan aliran keputusan dalam suatu sistem atau proses. *Activity* *diagram* sangat berguna untuk menggambarkan proses dinamis dalam sistem, seperti aliran kontrol dari satu aktivitas ke aktivitas lain dan bagaimana keputusan diambil di sepanjang proses.

*Activity diagram voting creation*



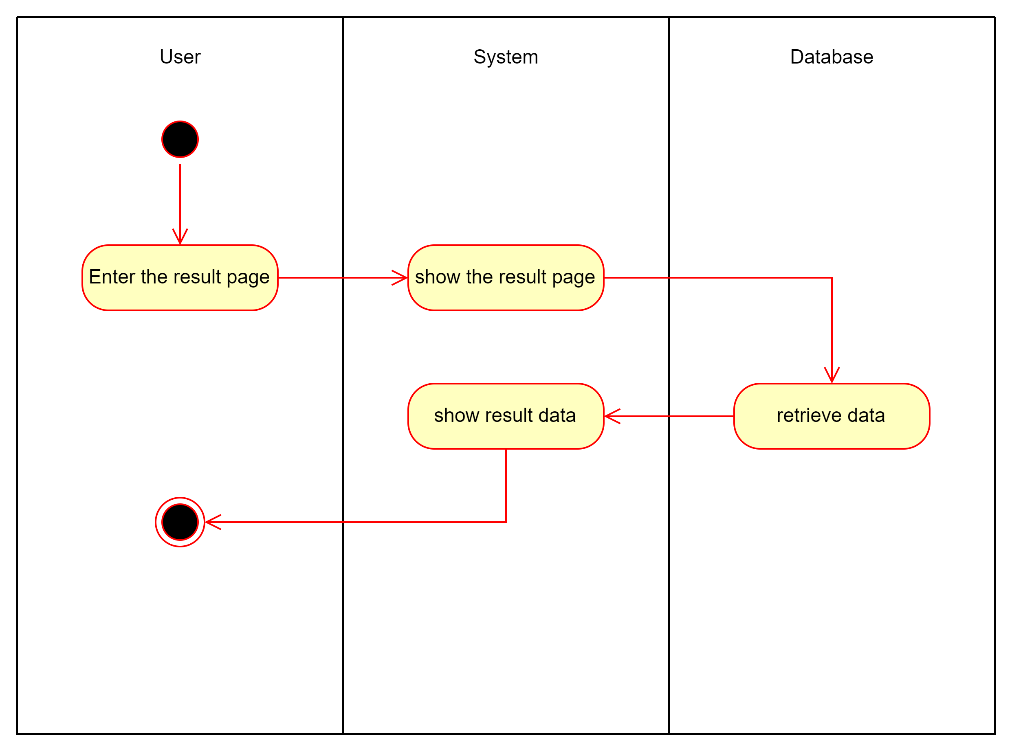
#### Gambar 4.3 *voting creation*

*Activity diagram voting creation*



#### Gambar 4.4 *voting creation*

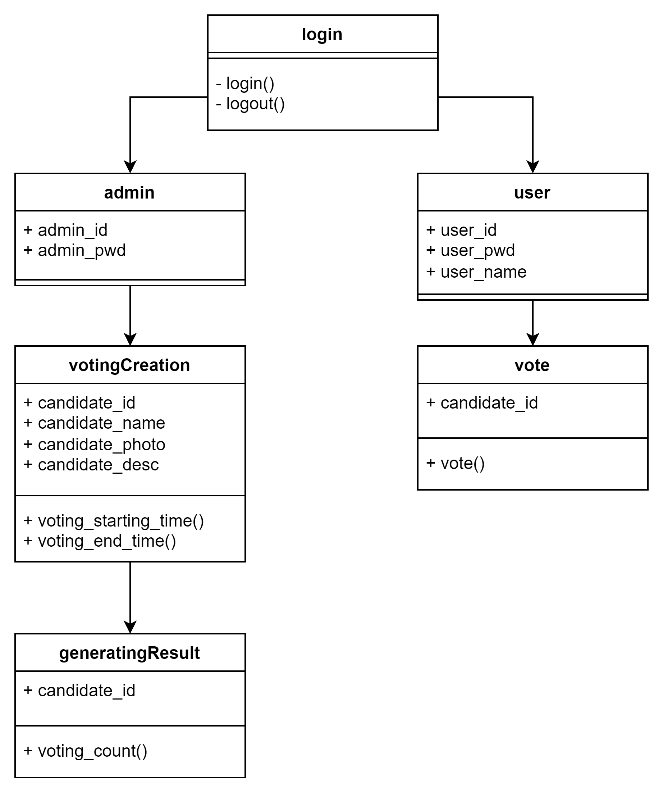
*Activity diagram generate result*



#### Gambar 4.5 *generate result*

### **4.2.4. *Class Diagram***

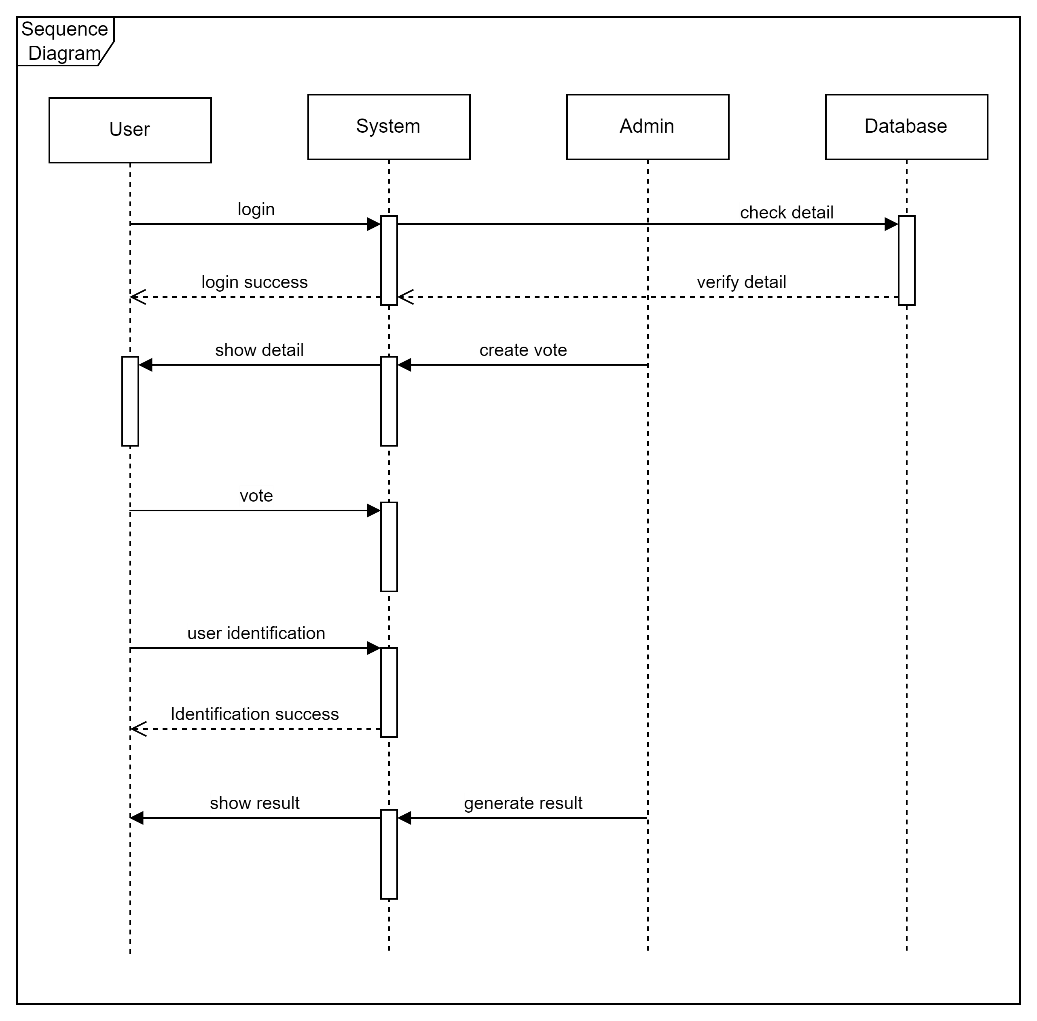
*Class diagram* atau diagram kelas adalah salah satu jenis diagram struktur pada *UML* yang menggambarkan dengan jelas struktur serta deskripsi *class*, atribut, metode, dan hubungan dari setiap objek. *Class diagram* ini bersifat statis, dalam artian diagram ini bukan menjelaskan apa yang terjadi jika kelas-kelasnya berhubungan, melainkan menjelaskan hubungan apa yang terjadi. *Class diagram* ini emiliki beberapa fungsi, fungsi utamanya yaitu menggambarkan struktur dari sebuah sistem.



#### Gambar 4.6 *Class Diagram*

### **4.2.4. *Sequence Diagram***

*Sequence diagram* atau diagram urutan adalah sebuah diagram yang digunakan untuk menjelaskan dan menampilkan interaksi antar objek-objek dalam sebuah sistem secara terperinci. Selain itu *sequence diagram* juga akan menampilkan pesan atau perintah yang dikirim, beserta waktu pelaksanaannya. Tujuan utama dari pembuatan *sequence diagram* adalah untuk mengetahui urutan kejadian yang dapat menghasilkan output yang diinginkan. Selain itu, tujuan dari diagram urutan ini mirip dengan *activity diagram*, seperti menggambarkan alur kerja dari sebuah aktivitas, serta dapat menggambarkan aliran data dengan lebih detail, termasuk data atau perilaku yang diterima atau dikirimkan.

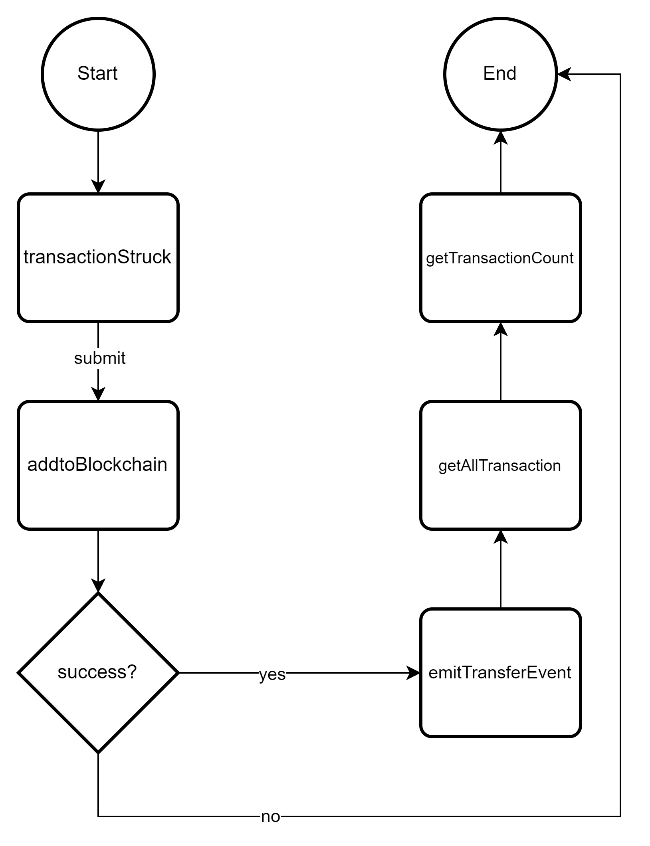


#### Gambar 4.7 *Sequence Diagram*

## **4.3. *Development* (Pengembangan)**

### **4.3.1. *Smart Contract***

*Smart contract* adalah transaksi yang berisi kode yang akan dieksekusi otomatis ketika kondisi dan persyaratan tertentu terpenuhi. *Smart contract* tidak membutuhkan intermediari seperti pengguna hukum atau pihak pengawas untuk menjamin perjanjian. *Smart* *contract* dapat mengatur dan mengatur transaksi, mengatur proses, dan mengelola aset digital dalam sistem yang tidak tergantung pada pihak tertentu. *Smart contract* ini ditulis dalam berbagai macam bahasa pemrograman, diantaranya *solidity.* *Solidity* memungkinkan pengembang untuk mengembangkan aplikasi yang kompatibel dengan *ethereum*. Setiap komputer dalam jaringan (atau “*node*”) menyimpan salinan semua *smart contract* yang ada dan statusnya saat ini bersama dengan *blockchain* dan data transaksi. Ketika *smart contract* menerima data dari pengguna, kodenya dieksekusi oleh semua *node* dalam dalam jaringan untuk mencapai konsensus tentang hasil dan aliran nilai yang dihasilkan. Inilah yang memungkinkan *smart contract* berjalan dengan aman tanpa otoritas pusat, bahkan ketika pengguna melakukan transaksi keuangan yang kompleks dengan entitas yang tidak dikenal. Untuk mengeksekusi *smart contract* di jaringan *Ethereum*, biasanya harus membayar biaya yang disebut “*gas*” (dinamakan demikian karena biaya ini membuat *blockchain* tetap berjalan).

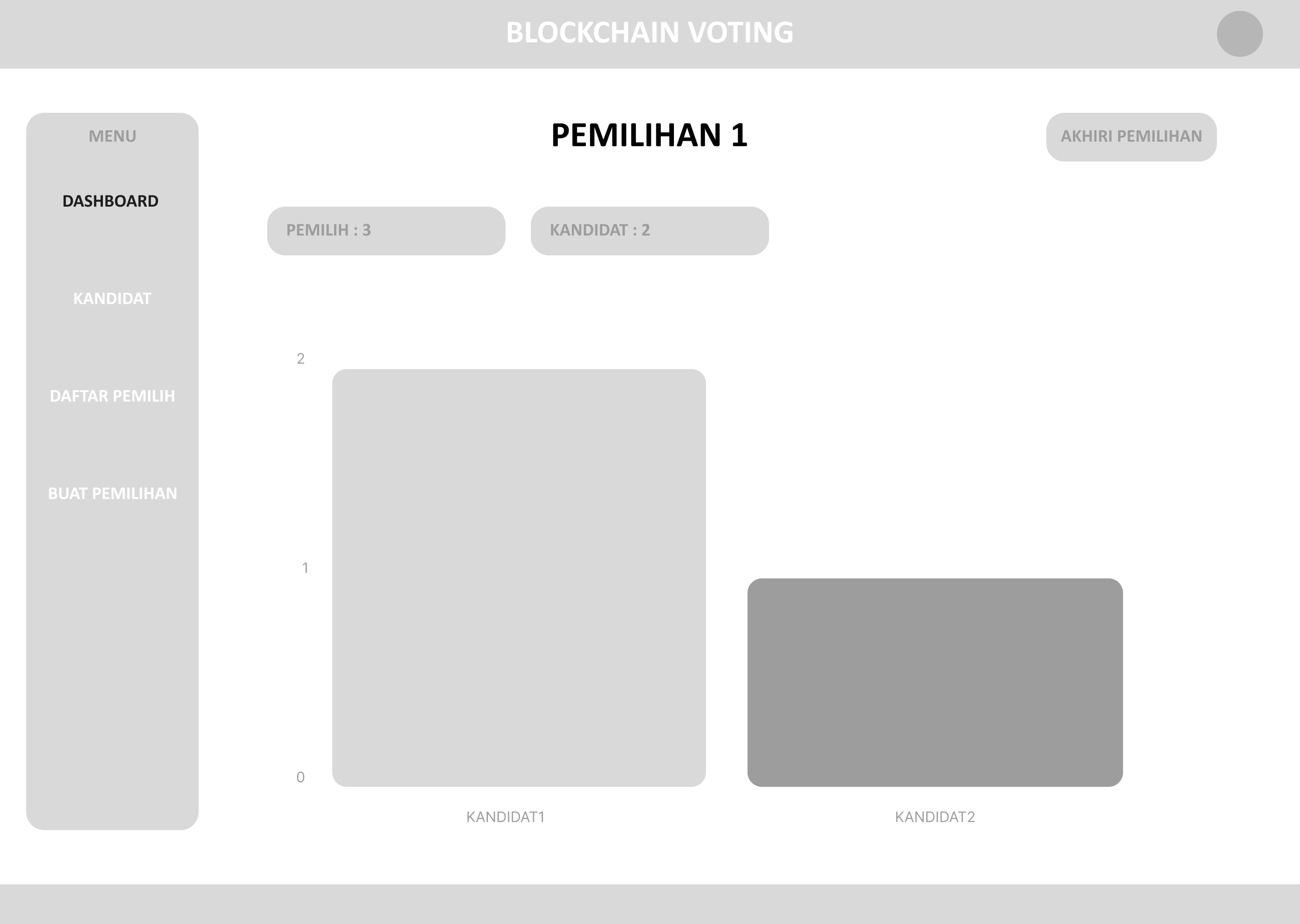


#### Gambar 4.8 *Smart Contract*

Berdasarkan gambar 4.7 Titik awal dari proses. Pada langkah ini, sistem siap menerima input untuk memulai proses transaksi. *transactionStruct* ini adalah langkah di mana transaksi (*voting*) didefinisikan dan siap untuk dicatat. Di sini, data seperti *receiver*, *user\_id*, *election\_id*, dan *candidate\_id* disiapkan. *addtoBlockchain* pada langkah ini, sistem menambahkan transaksi baru ke dalam *blockchain*, memperbarui *transactionCounter*, dan menyimpan transaksi ke dalam array *transactions*. Selanjutnya ada *decision* *node* yang menentukan apakah transaksi berhasil atau tidak, Jika transaksi berhasil, *eventTransfer* akan dipancarkan untuk memberitahu jaringan bahwa transaksi baru telah terjadi, mencatat rincian transaksi yang sudah disimpan., namun jiga gagal proses tidak akan dilanjutkan, dan transaksi akan berhakhir. Setelah transaksi dicatat, pengguna dapat memanggil fungsi *getAllTransaction* untuk mendapatkan semua transaksi yang tersimpan. Pengguna juga dapat memanggil fungsi *getTransactionCount* untuk mengetahui jumlah total transaksi yang telah dilakukan.

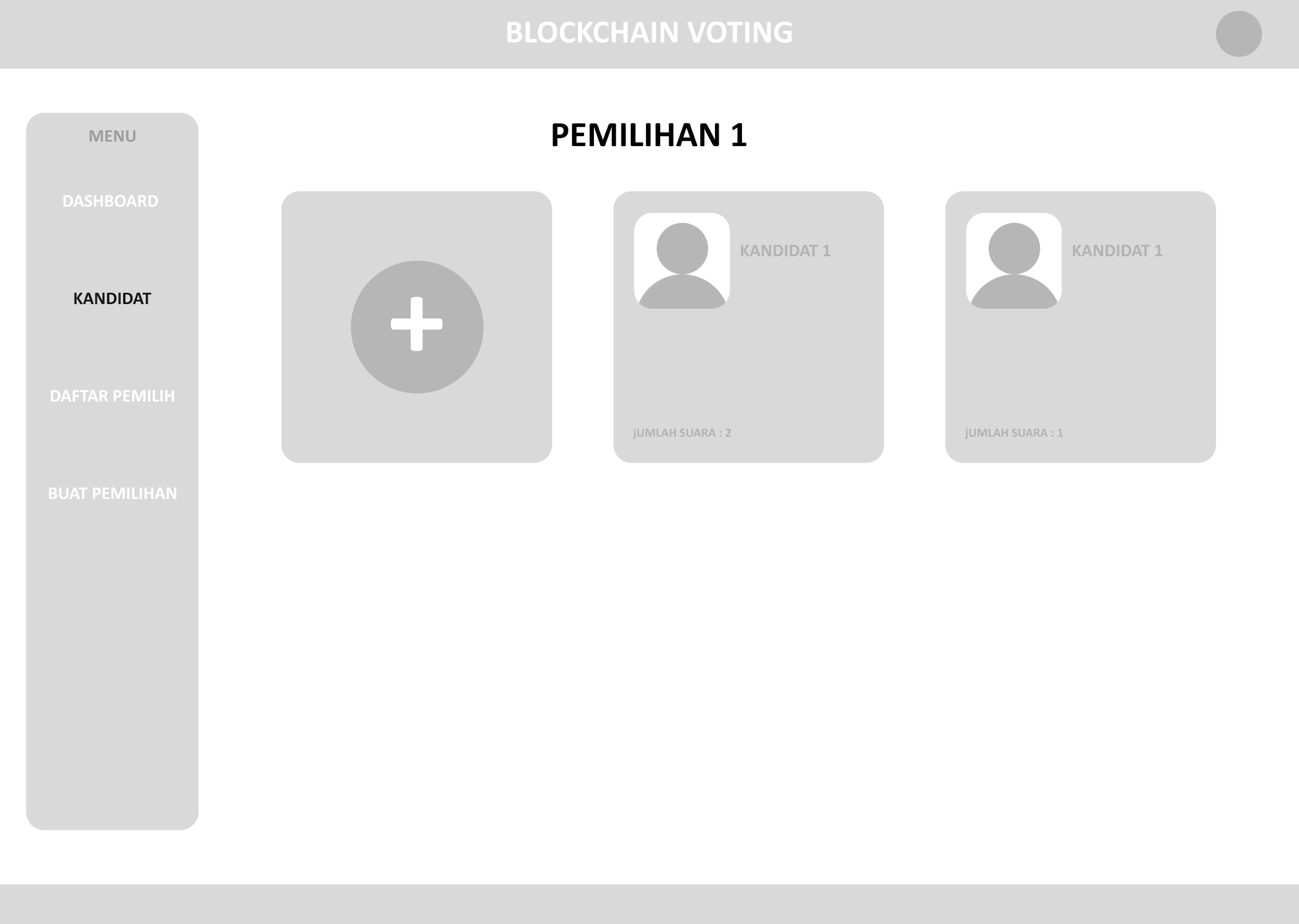
### **4.3.2. Pengembangan Antarmuka**

1. Halaman Admin-Dashboard

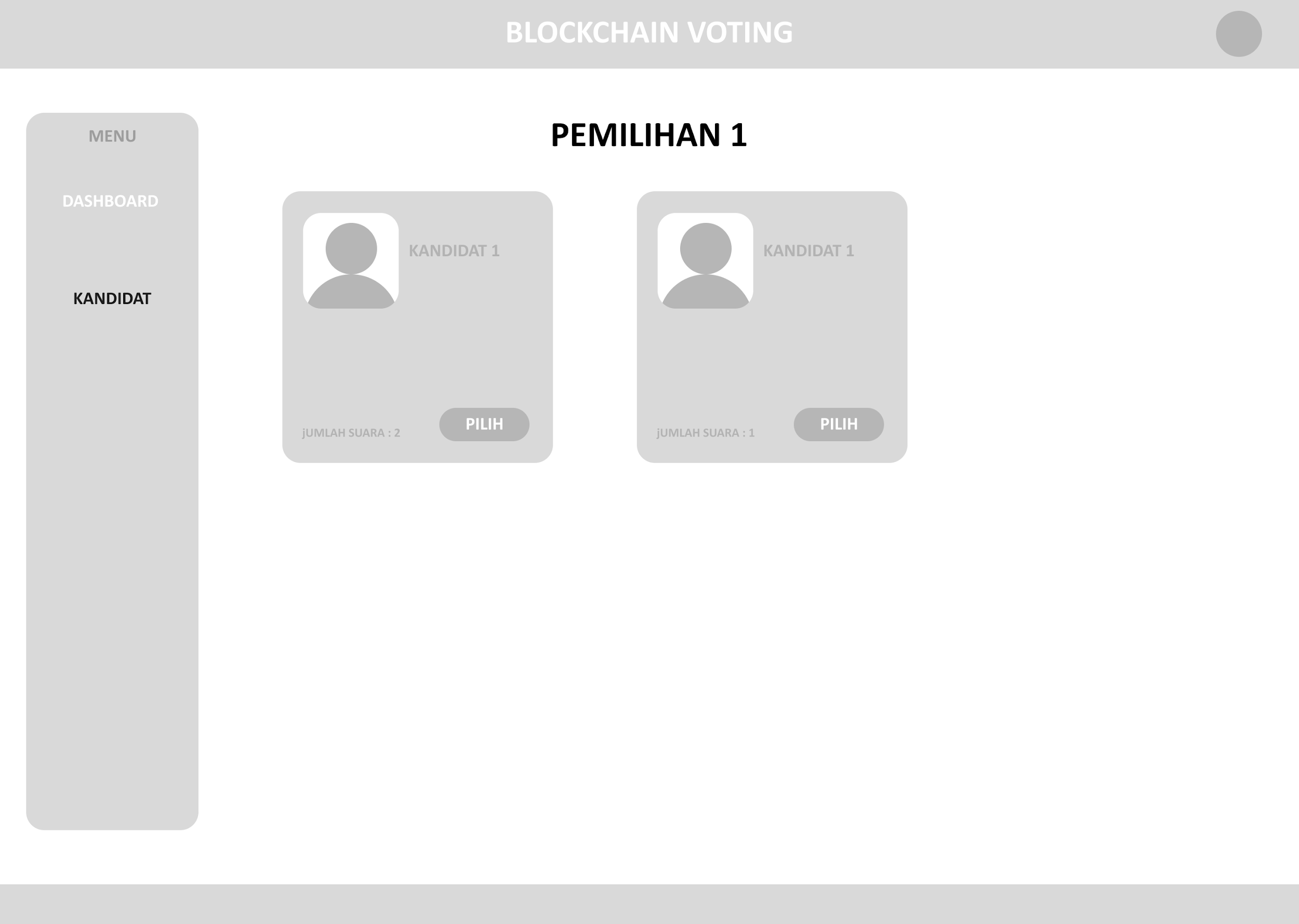


#### Gambar 4.9 Rancangan Antarmuka *Admin-Dashboard*

1. Halaman *Admin Voting Creation*



1. Halaman *User-Vote, Result*



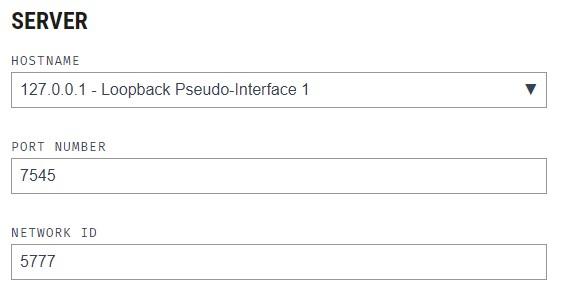
#### Gambar 4.10 Rancangan Antarmuka *User-Vote*

## **4.4. *Testing* (Pengujian)**

### **4.4.1. Pengujian *Smart Contract***

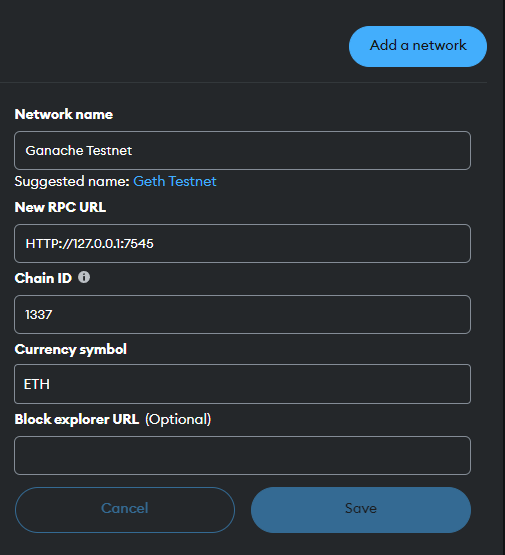
*Smart Contract Testing* bertujuan untuk memastikan bahwa kode *smart contract* yang ditulis dalam *Solidity* bekerja sesuai spesifikasi. Pengujian dilakukan dengan menggunakan *Node.js v.18.40, Truffle v5.11.5 , Ganache v2.7.1 , Solidity, dan web3.js.*

Untuk menginstall *truffle* bisa menggunakan *command* “npm install -g truffle” pada *terminal.* Lalu untuk menginstall ganache bisa dengan mengunjungi official website dan mengikuti instruksi yang tertera. Selanjutnya adalah melakukan konfigurasi ganache pada menu *setting*, seperti yang tertera pada gambar 4.8:



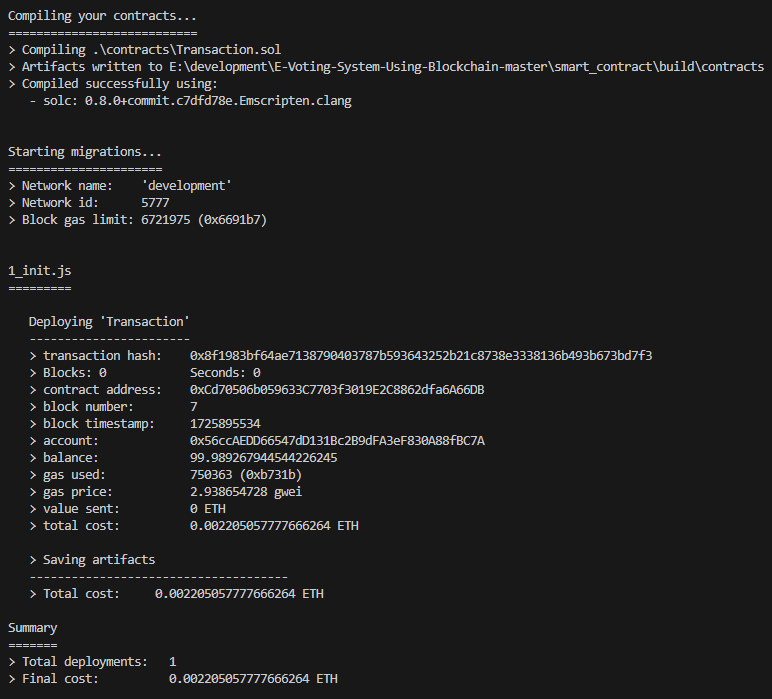
#### Gambar 4.11 *Ganache Server Detail*

Selanjutnya konfigurasi *metamask* untuk jaringan *local blockchain* seperti pada gambar 4.9:



#### Gambar 4.12 Konfigurasi *Metamask*

Setelah selesai konfigurasi *ganache* dan *metamask*, langkah selanjutnya adalah masuk ke direktori *smart contract* dan menjalankan *command* “*truffle migrate*” pada *terminal*. Perintah ini berfungsi untuk men-*deploy* *smart contract* ke jaringan *local blockchain*. Seperti pada gambar 4.10:

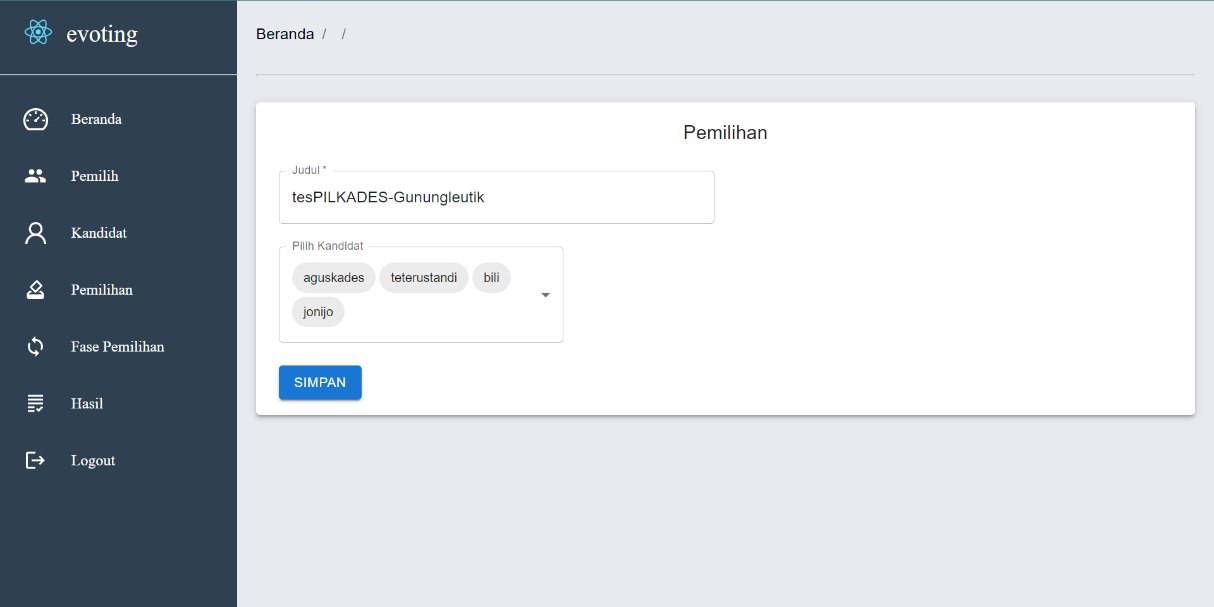


#### Gambar 4.13 *Truffle Migrate*

### **4.4.2. *Mock Election***

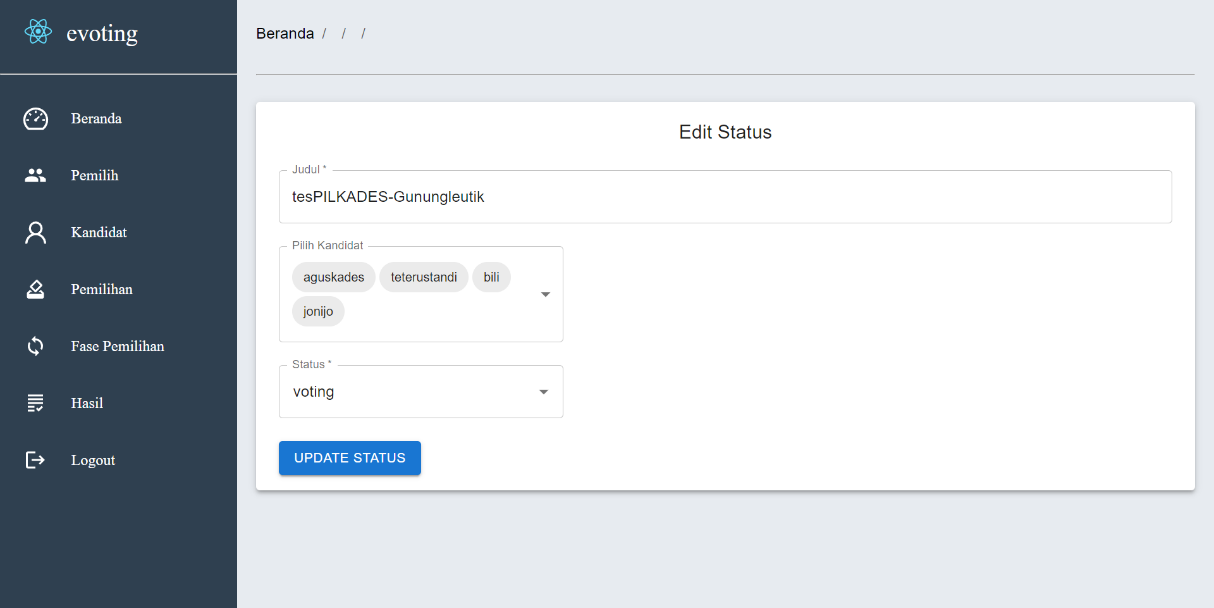
*Mock Election* adalah simulasi pemilihan elektronik yang dilakukan untuk menguji sistem dalam skenario nyata. Dalam uji coba ini, sejumlah pemilih melakukan pendaftaran, pemungutan suara, dan hasil pemungutan suara dihitung secara otomatis oleh sistem. Tujuannya adalah untuk menguji pengalaman pengguna, stabilitas sistem, dan kinerja secara keseluruhan.

1. Admin dapat menambahkan Pemilihan dalam sistem, dimana admin mengisi judul dan kandidat setelah klik tombol simpan, data pemilihan akan ditambahkan ke dalam database.



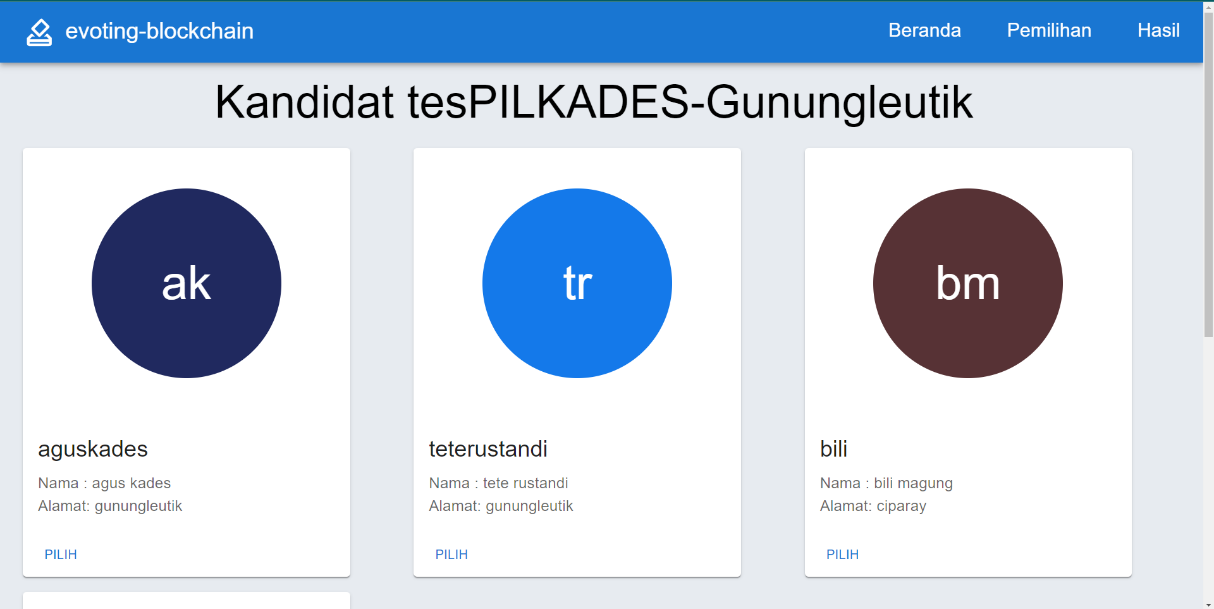
#### Gambar 4.14 *Add Election*

1. Admin dapat mengubah status fase pemilihan dimana ada tiga fase yaitu *init*, *voting* dan *counting*.



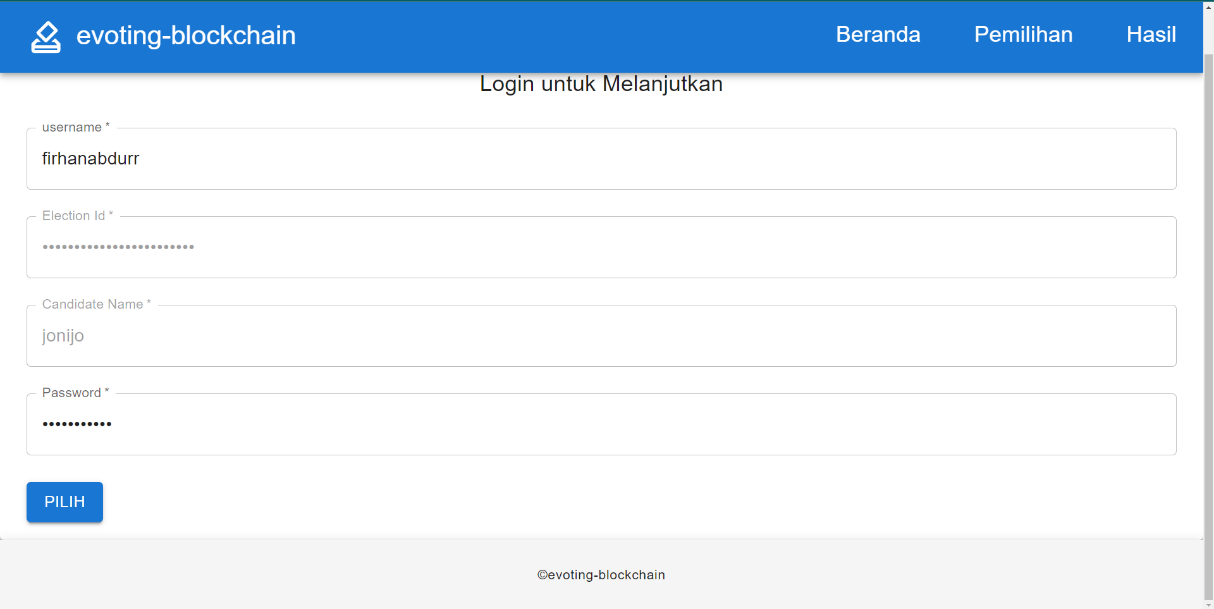
#### Gambar 4.15 *Add Phase*

1. Pada halaman detail pemilihan, pemilihdapat memilih para kandidat yang tersedia, dengan klik tombol pilih.



#### Gambar 4.16 *Election-detail*

1. Setelah pemilih memilih pada halaman pemilihan, pemilih akan diarahkan menuju halam verifikasi data diri, dan *user* memasukan *username* dan *password* untuk mengonfirmasi kandidat yang dipilihnya.



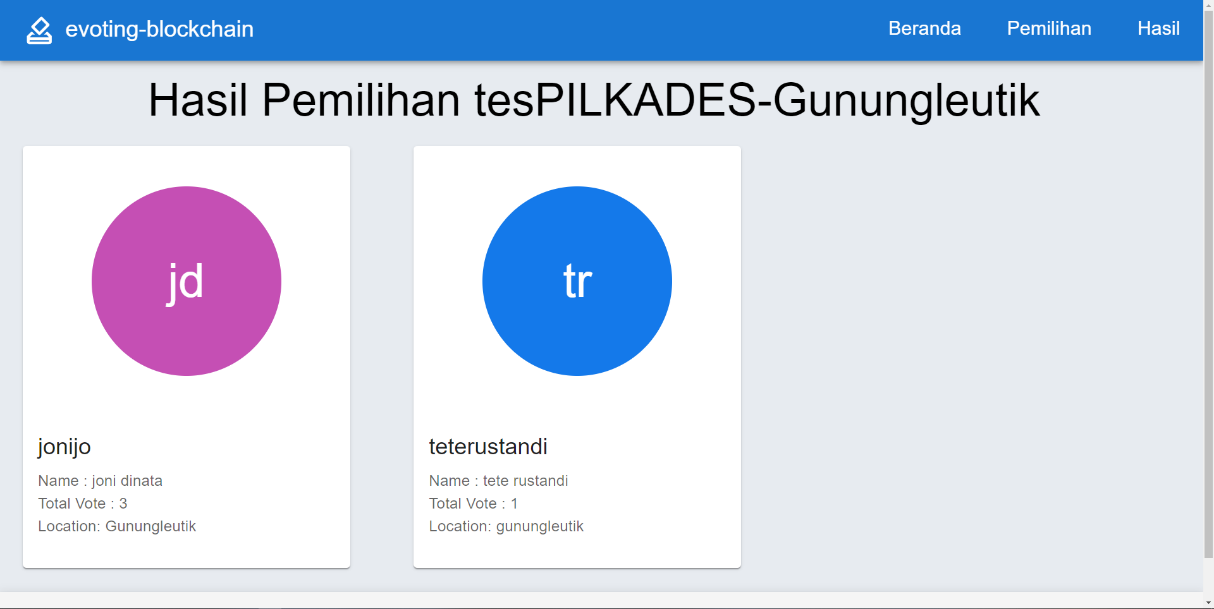
#### Gambar 4.17 *User Identification*

1. Setelah mengisi data verifikasi pemilih akan mendapati *pop-up* ekstensi *metamask* untuk mengonfirmasi transaksi dengan *ethereum blockchain*.



#### Gambar 4.18 *Metamask Confirmation*

1. Terakhir untuk melihat hasil pemilihan terdapat halaman hasil, yang berisi hasil pemilihan dan jumlah suara yang didapat.



#### Gambar 4.19 *Result*

BAB V SIMPULAN DAN SARAN

## **4.3. Kesimpulan**

Berdasarkan penelitian yang telah dilakukan mengenai Perancangan dan Implementasi Sistem Pemilihan Elektronik (*E-Voting*) Berbasis *Blockchain* Menggunakan *Solidity*, dapat disimpulkan bahwa sistem *e-voting* berbasis blockchain menawarkan solusi yang signifikan untuk mengatasi berbagai permasalahan yang sering dihadapi dalam pemilihan tradisional. Teknologi blockchain, dengan fitur desentralisasi dan keamanan berbasis kriptografi, mampu memberikan keamanan, transparansi, anonimitas, dan efisiensi yang lebih baik dibandingkan sistem manual. Pengujian melalui simulasi dan implementasi *smart contract* menunjukkan bahwa sistem dapat berjalan dengan baik dalam mencatat suara secara *real-time*, serta memastikan suara yang diberikan tidak dapat dimanipulasi setelah terekam di *blockchain*.

## **4.3. Saran**

Berdasarkan penelitian yang telah dilakukan mengenai Perancangan dan Implementasi Sistem Pemilihan Elektronik (E-Voting) Berbasis *Blockchain* Menggunakan *Solidity*, beberapa saran yang diperoleh untuk penelitian masa depan:

* + - 1. Pengembangan lebih lanjut, Diperlukan pengembangan lebih lanjut pada antarmuka pengguna untuk meningkatkan kemudahan penggunaan bagi pemilih yang kurang familiar dengan teknologi *blockchain*. Edukasi publik mengenai penggunaan dompet digital seperti *MetaMask* perlu ditingkatkan agar masyarakat lebih siap dalam menggunakan sistem ini.
      2. Skalabilitas sistem, Untuk memastikan sistem dapat digunakan dalam skala yang lebih besar seperti pemilihan umum nasional, perlu dilakukan uji coba pada jaringan *blockchain* yang lebih besar dan desentralisasi penuh. Hal ini akan memastikan bahwa sistem tetap responsif meskipun digunakan oleh jutaan pemilih khususnya di Indonesia.
      3. Kolaborasi dengan pemerintahan dan institusi terkait, Implementasi *e-voting* berbasis *blockchain* sebaiknya melibatkan kerjasama dengan pihak pemerintah, komisi pemilihan, serta ahli keamanan siber untuk memastikan bahwa sistem yang dibangun dapat memenuhi standar keamanan dan regulasi yang ada.
      4. Audit dan uji keamanan berkala, Mengingat pentingnya keamanan dalam sistem pemilihan, perlu dilakukan audit rutin terhadap smart contract dan infrastruktur blockchain yang digunakan. Hal ini penting untuk memastikan bahwa sistem tetap aman dari potensi serangan siber.

# **LAMPIRAN**

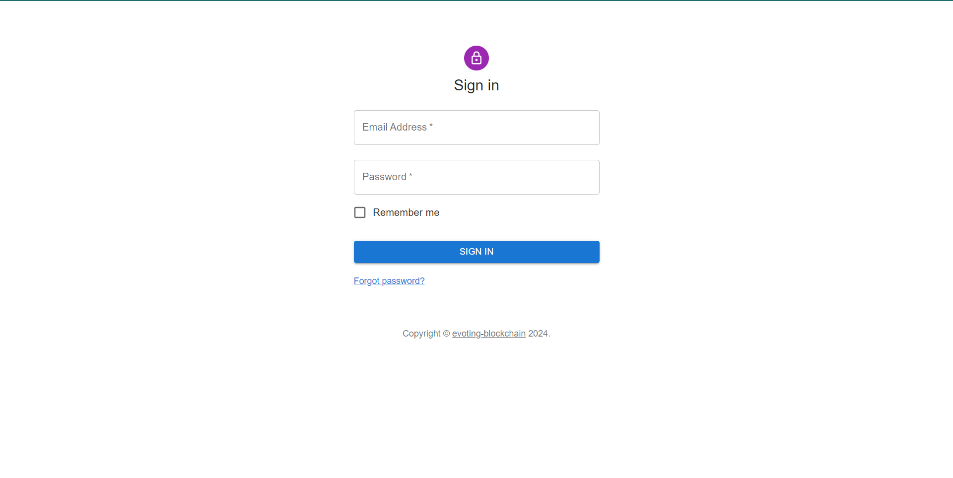
Lampiran 1. Lembar Bimbingan Skripsi

Lampiran 1. Surat Ijin Penelitian Lapangan

Lampiran 1. Daftar Pertanyaan Kuisioner

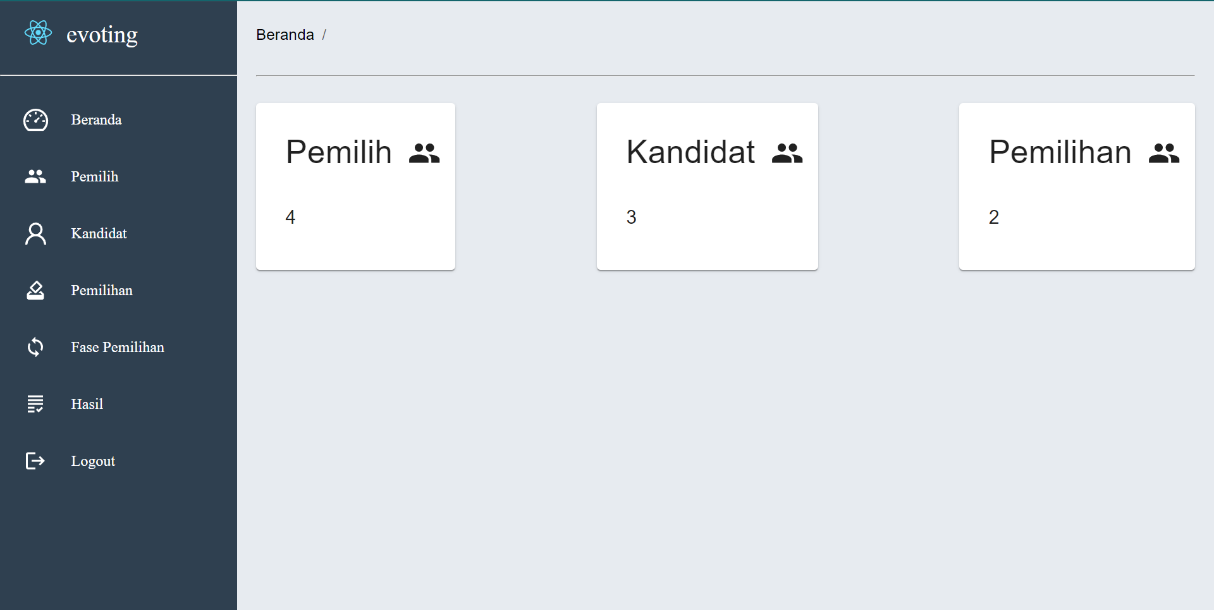
Lampiran 1. Hasil

1. Halaman *login* untuk admin.



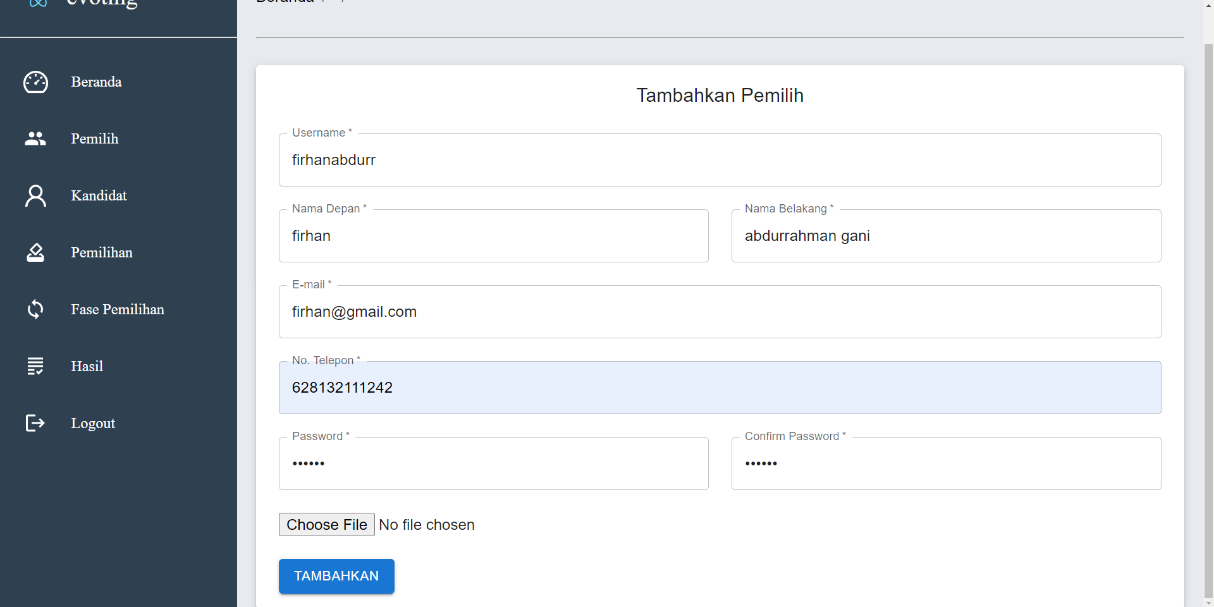
#### Gambar 4.18 *Admin-login*

1. Ditampilkan *dahsboard admin* dimana semua informasi seperti jumlah pemilih, kandidat, dan pemilihan yang tersedia pada sistem, serta di sampingnya ada menu-menu seperti Pemilih , kandidat, pemilihan, fase pemilihan, dan hasil pemilihan.



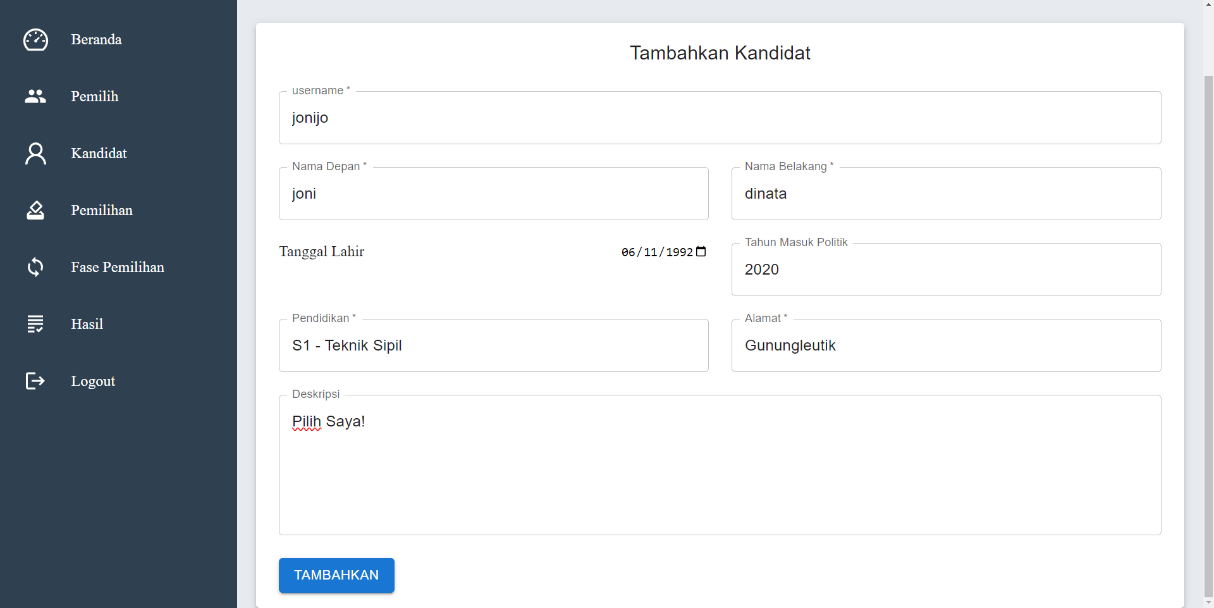
#### Gambar 4.19 *Admin-dahsboard*

1. Admin dapat menambahkan Pemilih dalam sistem dimana admin harus mengisi detail seperti NIK, nama depan dan detail lainnya setelah klik tambah pengguna orang akan mendapatkan nama pengguna dan *password* dalam *email* yang dimasukkan dalam formulir yang diberikan.



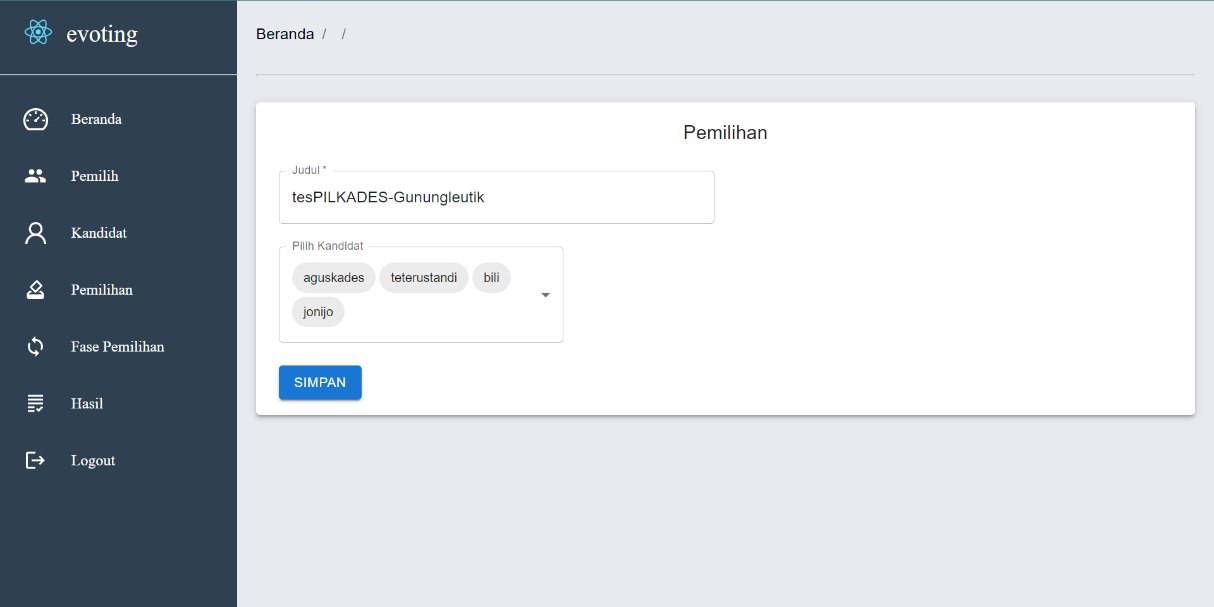
#### Gambar 4.20 *Add User*

1. Admin dapat menambahkan Kandidat dalam sistem dimana admin harus mengisi detail seperti NIK, nama depan dan detail lainnya setelah klik Tambahkan, data kadidat akan ditambahkan ke dalam *database*.



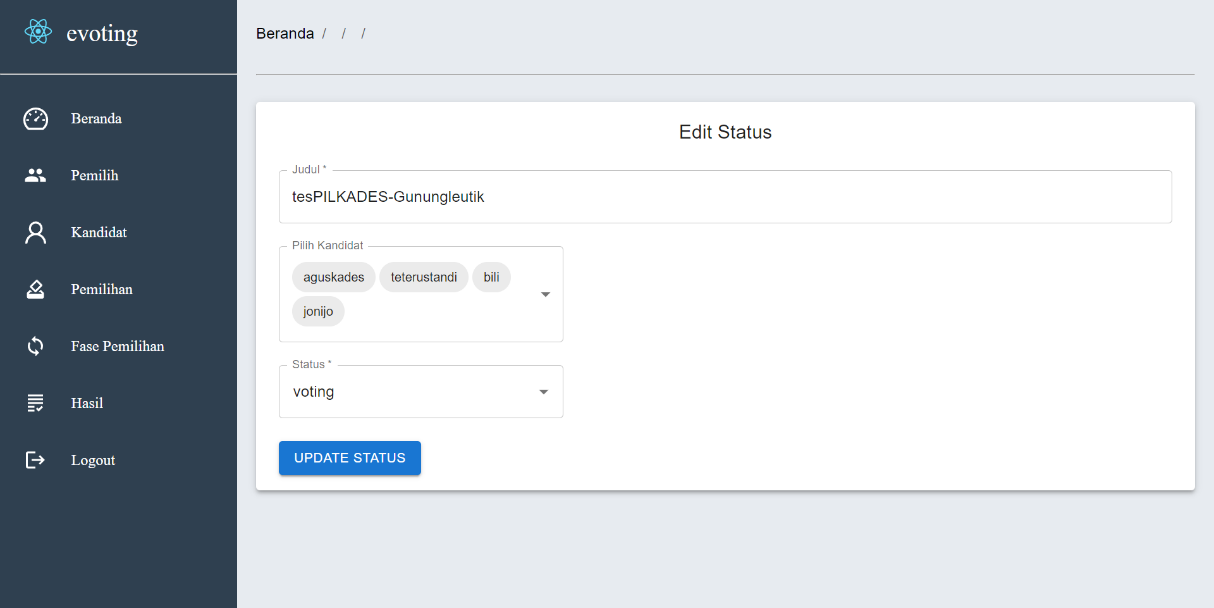
#### Gambar 4.21 *Add Candidate*

1. Admin dapat menambahkan Pemilihan dalam sistem, dimana admin mengisi judul dan kandidat setelah klik tombol simpan, data pemilihan akan ditambahkan ke dalam database.



#### Gambar 4.22 *Add Election*

1. Admin dapat mengubah status fase pemilihan dimana ada tiga fase yaitu *init*, *voting* dan *counting*.



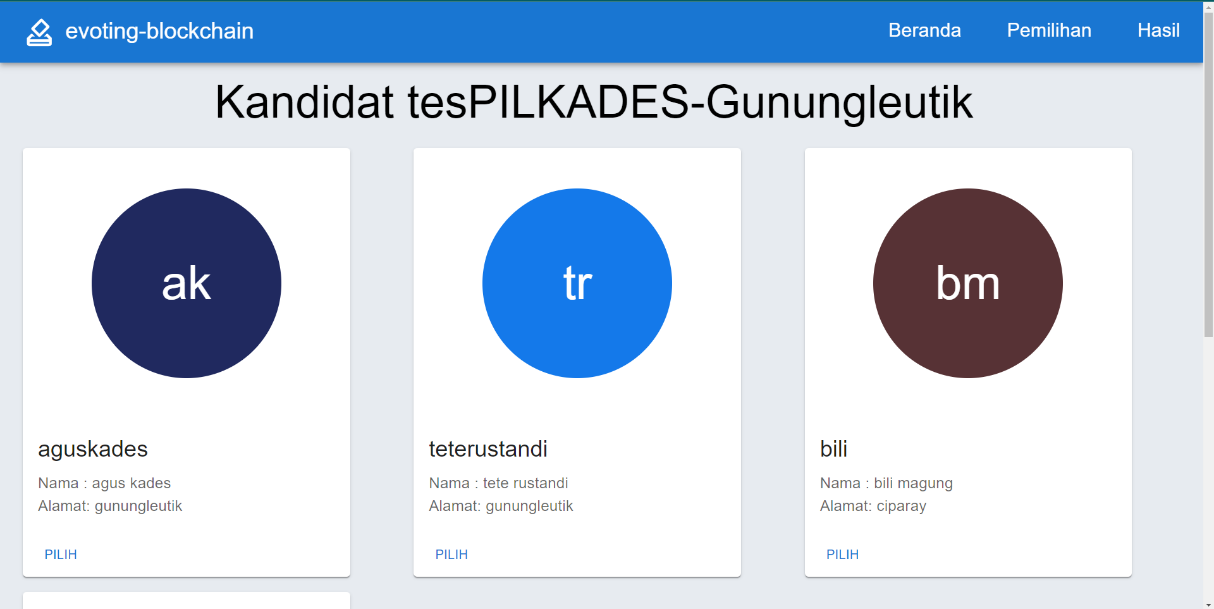
#### Gambar 4.23 *Add Phase*

1. Pada halaman Pemilihan, pemilih dapat melihat pemilihan yang sedang berlangsung.



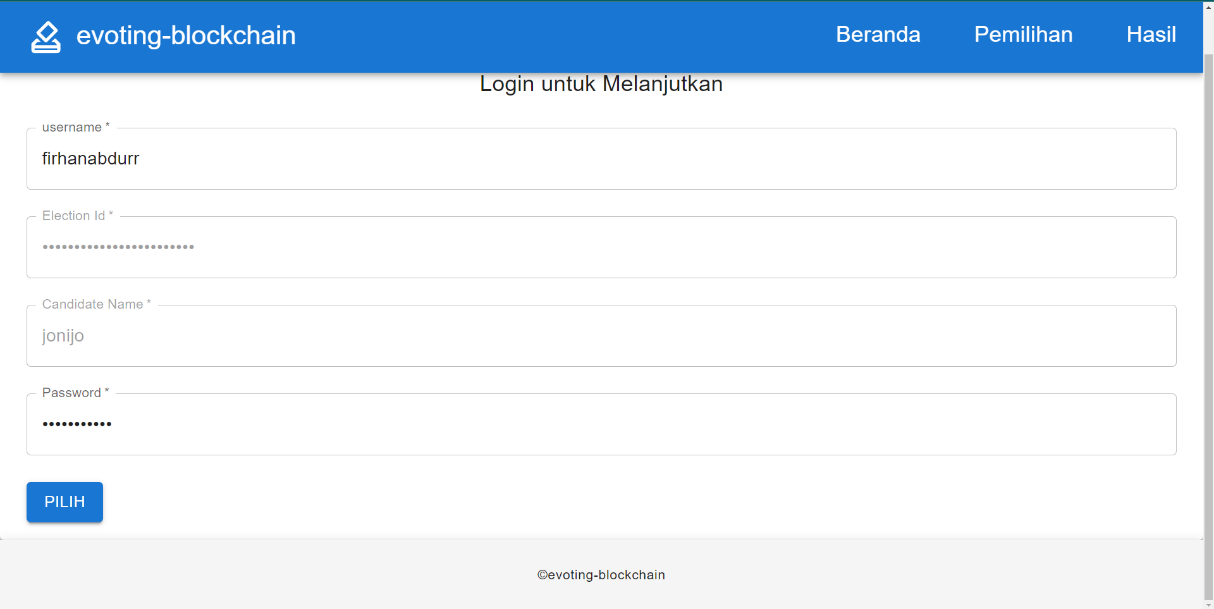
#### Gambar 4.24 *Election*

1. Pada halaman detail pemilihan, pemilihdapat memilih para kandidat yang tersedia, dengan klik tombol pilih.



#### Gambar 4.25 *Election-detail*

1. Setelah pemilih memilih pada halaman pemilihan, pemilih akan diarahkan menuju halam verifikasi data diri, dan *user* memasukan *username* dan *password* untuk mengonfirmasi kandidat yang dipilihnya.



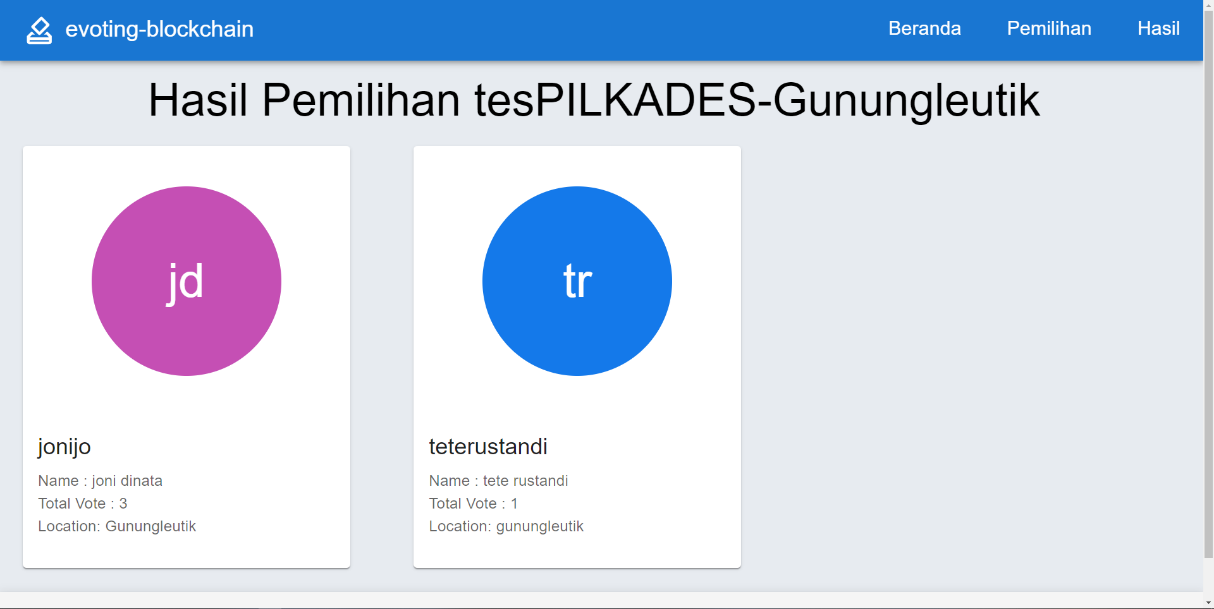
#### Gambar 4.26 *User Identification*

1. Setelah mengisi data verifikasi pemilih akan mendapati *pop-up* ekstensi *metamask* untuk mengonfirmasi transaksi dengan *ethereum blockchain*.



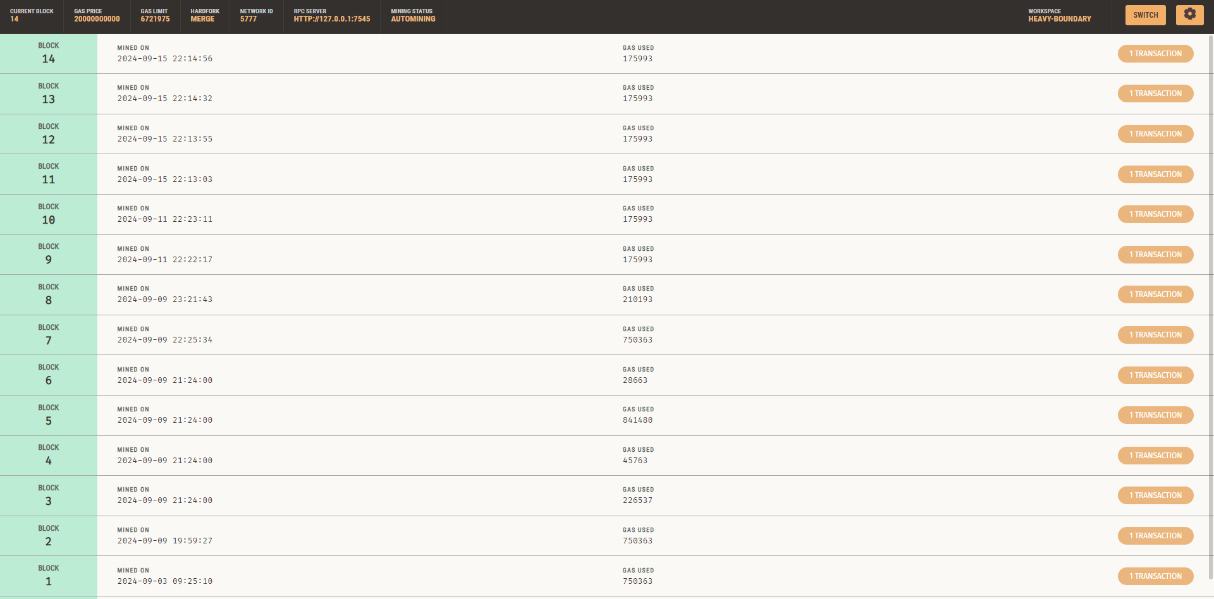
#### Gambar 4.27 *Metamask Confirmation*

1. Terakhir untuk melihat hasil pemilihan terdapat halaman hasil, yang berisi hasil pemilihan dan jumlah suara yang didapat.

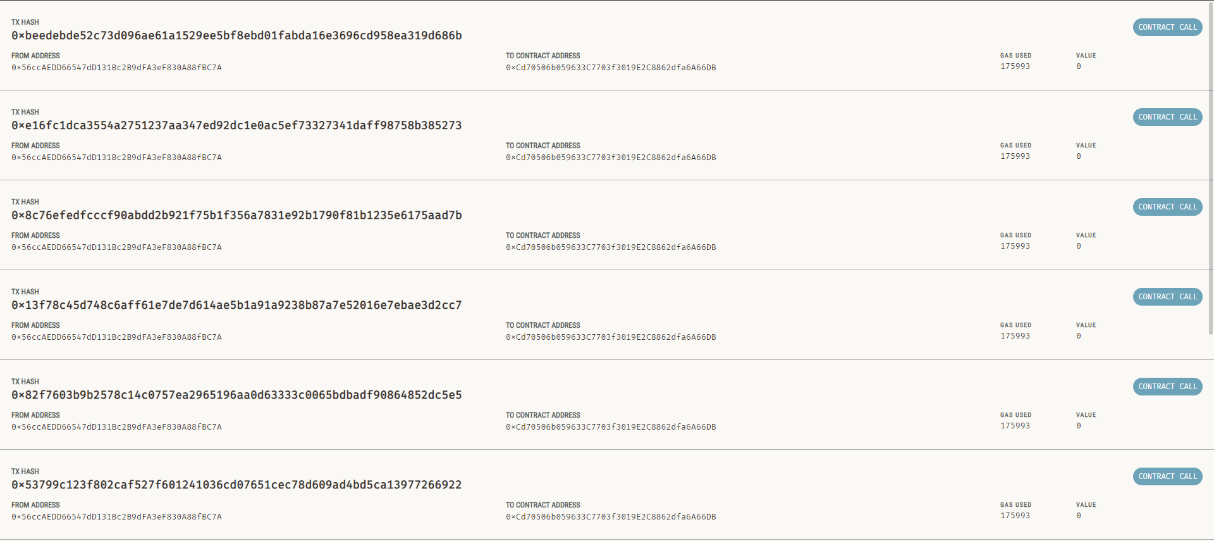


#### Gambar 4.28 *Result*

1. Untuk keperluan audit, setiap transaksi direkam ke dalam jaringan blockchain, gambar 4.29 dan 4.30 merupakan rincian transaksi yang sudah terenkripsi menggunakan kriptografi *blockchain*.



#### Gambar 4.29 *Mining Block*



#### Gambar 4.30 *Record Transaction*

Lampiran 1. *Smart Contract*

|  |
| --- |
| pragma solidity ^0.8.0;  contract Transaction{      uint256 transactionCounter;      event Transfer(address from,address receiver,string user\_id,string election\_id,string candidate\_id,uint timestamp);      struct TransactionStruct {          address from;          address receiver;          string user\_id;          string election\_id;          string candidate\_id;          uint timestamp;      }      TransactionStruct[] transactions;      function addToBlockchain(address payable receiver,string memory user\_id,string memory election\_id,string memory candidate\_id) public {          transactionCounter+=1;          transactions.push(TransactionStruct(msg.sender,receiver,user\_id,election\_id,candidate\_id,block.timestamp));          emit Transfer(msg.sender,receiver,user\_id,election\_id,candidate\_id,block.timestamp);      }      function getAllTransaction() public view returns (TransactionStruct[] memory){          return transactions;      }      function getTransactionCount() public view returns (uint256){          return transactionCounter;      }  } |

Lampiran 1. *Source Code Program*

Code program untuk add user

|  |
| --- |
| export const users = {    getUsers: async (req, res) => {      try {        const tmp = await User.find();        return res.status(201).send(tmp);      } catch (e) {        return res.status(500).send("Error");      }    },    getUser: async (req, res) => {      try {        const tmp = await User.findById(req.params.id);        return res.status(201).send(tmp);      } catch (e) {        console.log(e);        return res.status(500).send("Error!");      }    },    getUserByName: async (req, res) => {      try {        const tmp = await User.find({ username: req.params.id });        return res.status(201).send(tmp);      } catch (e) {        console.log(e);        return res.status(500).send("Error!");      }    },    delete: async (req, res) => {      try {        const tmp = await User.findByIdAndDelete(req.params.id);        const isPhotoDeleted = users.deleteUserProfile(tmp);        if (isPhotoDeleted) {          return res            .status(201)            .send("Election and photo file deleted successfully");        } else {          return res.status(500).send("Error deleting photo file");        }      } catch (e) {        console.log(e);        return res.status(500).send("Error!");      }    },    edit: async (req, res) => {      const tmp = await User.findById(req.params.id);      const isPhotoDeleted = users.deleteUserProfile(tmp);      if (!isPhotoDeleted) {        return res.status(500).send("Error updating User");      }      upload(req, res, async function (err) {        if (err instanceof multer.MulterError) {          return res.status(500).json(err);        } else if (err) {          return res.status(500).json(err);        }        try {          const user = {            username: req.body.username,            email: req.body.email,            mobile: req.body.mobile,            fname: req.body.fname,            lname: req.body.lname,          };          const tmp = await User.findByIdAndUpdate(req.params.id, user);          return res.status(201).send("User Updated Successfully");        } catch (e) {          console.log(e);          return res.status(500).send("error");        }      });    },  }; |

Kode ini adalah kumpulan metode untuk mengelola operasi terkait *User*, termasuk mengambil, menghapus, dan mengedit profil user di *database* *MongoDB* dengan menggunakan model *User*. *getUsers(req, res):* Mendapatkan semua user berdasarkan id dari database. Jika berhasil, mengembalikan daftar user dengan status 201. Jika terjadi error, mengembalikan status 500.

Code program untuk add candidate

|  |
| --- |
| export const candidateRegister = {    validator: async (req, res, next) => {      next();    },    controller: async (req, res) => {      const candidate = await Candidate.create({        username: req.body.username,        firstName: req.body.firstName,        lastName: req.body.lastName,        dob: req.body.dob,        qualification: req.body.qualification,        join: req.body.join,        location: req.body.location,        description: req.body.description,      });      return res.status(201).send("Candidate Added");    },  };  export const candidates = {    getCandidates: async (req, res) => {      const data = await Candidate.find();      return res.status(201).send(data);    },    register: async (req, res) => {      const candidate = await Candidate.create({        username: req.body.username,        firstName: req.body.firstName,        lastName: req.body.lastName,        dob: req.body.dob,        qualification: req.body.qualification,        join: req.body.join,        location: req.body.location,        description: req.body.description,      });      return res.status(201).send("Candidate Added");    },    getCandidate: async (req, res) => {      const data = await Candidate.findOne({ username: req.params.username });      if (data == null) {        return res.status(500).send("Candidate Not Found");      }      return res.status(201).send(data);    },    delete: async (req, res) => {      try {        const data = await Candidate.findByIdAndDelete(req.params.id);        return res.status(201).send("Candidate Deleted Successfully");      } catch (e) {        return res.status(500).send("Error");      }    },  }; |

Kode ini merupakan kumpulan fungsi yang digunakan untuk mengelola data kandidat dalam aplikasi. Fungsi-fungsi ini mengelola operasi seperti menambah, mengambil, dan menghapus data kandidat.

Code program untuk election

|  |
| --- |
| export const elections = {    controller: async (req, res) => {      try {        const tmp = await Election.find();        return res.status(201).send(tmp);      } catch (e) {        return res.status(500).send("Error");      }    },    register: async (req, res) => {      try {        const newElection = await Election.create({          name: req.body.name,          candidates: req.body.candidates,        });        return res.status(201).send("Election Successfully Added");      } catch (e) {        return res.status(500).send("Internal Error" + e);      }    },    getElection: async (req, res) => {      try {        const data = await Election.findById(req.params.id);        return res.status(201).send(data);      } catch (e) {        return res.status(500).send("Error");      }    },    voting: async (req, res) => {      try {        const tmp = await Election.find({ currentPhase: "voting" });        return res.status(201).send(tmp);      } catch (e) {        return res.status(500).send("Error");      }    },    result: async (req, res) => {      try {        const tmp = await Election.find({ currentPhase: "result" });        return res.status(201).send(tmp);      } catch (e) {        return res.status(500).send("Error");      }    },    delete: async (req, res) => {      try {        const tmp = await Election.findByIdAndDelete(req.params.id);        return res.status(201).send("Election Deleted Successfully");      } catch (e) {        return res.status(500).send("Error");      }    },  }; |

Kode ini berisi fungsi-fungsi untuk mengelola *election,* didalamnya ada fungsi controller untuk mengambil semua data pemilihan yang ada pada database menggunakan *Election.find(),* ada juga *register* untuk mendaftrakan pemilihan baru dengan memasukan judul dan daftar kandidat. fungsi *voting* mengambil semua pemilihan yang berada pada fase *voting*. Fungsi *result* mengambil semua pemilihan yang berada pada fase *result*.

Code program untuk add phase

|  |
| --- |
| export const phase = {    controller: async (req, res) => {      const data = await Election.findByIdAndUpdate(req.params.id, {        currentPhase: req.body.currentPhase,      });      return res.status(201).send(data);    },  }; |

Kode ini berfungsi untuk memperbarui fase pemilihan menggunakan currenPhase yang diambil dari req.body.

DAFTAR PUSTAKA

[1] Hardjaloka, L., & Simarmata, V. M. (n.d.). *E-Voting: Kebutuhan vs. Kesiapan (Menyongsong) E-Demokrasi*.

[2] Falah, A. I., Rheza, K., & Adinegoro, R. (n.d.). PELUANG DAN TANTANGAN ADOPSI E-VOTING INDIA DALAM PEMILIHAN KEPALA DAERAH DI INDONESIA. In *Humaniora Dan Kebijakan Publik* (Vol. 5).

[3] *Wood, Gavin. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER EIP-150 REVISION*. (n.d.).

[4] Wu, Kean & Liu, Manlu & Xu, Jennifer. (2019). How Will Blockchain Technology Impact Auditing and Accounting: Permissionless Vs. Permissioned Blockchain. Current Issues in Auditing. 13. 10.2308/ciia-52540.

[5] Setiawan Restu Aji, and Wahyuningdiah Trisari Harsanti Putri. “Implementasi Teknologi Blockchain Dalam Aplikasi E-Voting Berbasis Mobile.” *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, vol. 14, no. 2, 1 Dec. 2023,<https://doi.org/10.31849/digitalzone.v14i2.16682>.

[6] Hutahaean, J. (2015). Konsep Sistem Informasi. Deepublish. https://books.google.co.id/books?id=o8LjCAAAQBAJ

[7] Bhutta, Muhammad Nasir Mumtaz, et al. “A Survey on Blockchain Technology: Evolution, Architecture and Security.” *IEEE Access*, vol. 9, no. 2169-3536, 2021, pp. 1–1,<https://doi.org/10.1109/access.2021.3072849>.

[8] Zheng, Zibin, et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.” *2017 IEEE International Congress on Big Data (BigData Congress)*, June 2017, https://doi.org/10.1109/bigdatacongress.2017.85. Accessed 29 Mar. 2024.

[9] H Purwantoro and M Y Wibowo, Teknologi Blockchain dan Cara Kerjanya. APTIKOM, 2020.

[10] M.Ilyas Gultom, M., & Saripurna, D. (2019). Perancangan Sistem Keamanan Aplikasi Evoting Untuk Pemilihan Ketua Badan Eksekutif Mahasiswa Fakultas Teknik UISU Dengan Menggunakan Algoritma MD5. Algoritma : Jurnal Ilmu Komputer Dan Informatika, 3(2), 70.<https://doi.org/10.30829/algoritma.v3i2.6438>

[11] Ben Ayed, A. (2017). A Conceptual Secure Blockchain Based Electronic voting System. International Journal of Network Security & Its Applications, 9(3), 01–09. https://doi.org/10.5121/ijnsa.2017.9301

[12] Andreas M Antonopoulos and Dr Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps 1st Edition, 1st ed. O’Reilly Media, 2018.

[13] Fadli, Fajri, et al. *Electronic Voting Using Decentralized System Based on Ethereum Blockchain*. 1 Mar. 2020,<https://doi.org/10.32409/jikstik.19.1.2718>.

[14] Curran, Kevin. “E-Voting on the Blockchain.” *The Journal of the British Blockchain Association*, vol. 1, no. 2, 4 Dec. 2018, pp. 1–6,<https://doi.org/10.31585/jbba-1-2-(3)2018>.

[15] Adekeye, Taiwo. (2023). Implementing a secure electronic voting system using Blockchain smart contract. 10.13140/RG.2.2.27008.10242.

[16] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[17] Jafar, Uzma, et al. “Blockchain for Electronic Voting System—Review and Open Research Challenges.” Sensors, vol. 21, no. 17, 31 Aug. 2021, p. 5874, <https://doi.org/10.3390/s21175874>.

[18] Kshetri, Nir, and Jeffrey Voas. “Blockchain-Enabled E-Voting.” IEEE Software, vol. 35, no. 4, July 2018, pp. 95–99, <https://doi.org/10.1109/ms.2018.2801546>.

[19] Mizzi, Jerome, and Frankie Inguanez. “Blockchain Based E-Voting System.” Journal of E-Technology, vol. 9, no. 2, 1 May 2018, p. 44, <https://doi.org/10.6025/jet/2018/9/2/44-48>.

[20] Shahzad, Basit, and Jon Crowcroft. “Trustworthy Electronic Voting Using Adjusted Blockchain Technology.” IEEE Access, vol. 7, 2019, pp. 24477–24488, <https://doi.org/10.1109/access.2019.2895670>.

[21] ---. “Blockchain Challenges and Opportunities: A Survey.” International Journal of Web and Grid Services, vol. 14, no. 4, 2018, p. 352, <https://doi.org/10.1504/ijwgs.2018.095647>.

[22] “Use of E-Voting around the World | International IDEA.” Www.idea.int, [www.idea.int/news-media/media/use-e-voting-around-world](http://www.idea.int/news-media/media/use-e-voting-around-world).

[23] Mohanta, Bhabendu & Panda, Soumyashree & Jena, Debasish. (2018). An Overview of Smart Contract and Use Cases in Blockchain Technology. 10.1109/ICCCNT.2018.8494045.

[24] M. -V. Vladucu, Z. Dong, J. Medina and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," in IEEE Access, vol. 11, pp. 23293-23308, 2023, doi: 10.1109/ACCESS.2023.3253682.

[25] Juliarto Rendi, “UML” Diakses: 28 September 2024. [Daring]. Tersedia pada: <https://www.dicoding.com/blog/apa-itu-uml/>

[26] Setiawan Rony, “konsep agile pada software development” Diakses: 28 September 2024. [Daring]. Tersedia pada: <https://www.dicoding.com/blog/konsep-agile-pada-software-development/>

[27] Salman, S. A. B., Al-Janabi, S., & Sagheer, A. M. (2022). A Review on E-Voting Based on Blockchain Models. *Iraqi Journal of Science*, 1362-1375.