Model Sistem Voting Digital Berbasis Blockchain dengan Zero-Knowledge Proof untuk Pemilihan yang Transparan dan Terdesentraliasi

Dora Bernadisman[1]✉, Dewi Sahara Nasution[2], Deni Murdiani[3]
[1-3]Universitas Saintek Muhammadiyah, Indonesia

✉Corresponding Author: dorabernadisman@gmail.com

ABSTRAK

Sistem pemungutan suara (*voting*) merupakan komponen penting dalam proses demokrasi yang menuntut tingkat keamanan, transparansi, dan kepercayaan publik yang tinggi. Namun, sistem voting konvensional maupun digital terpusat masih menghadapi berbagai permasalahan, seperti kerentanan terhadap manipulasi data, kurangnya transparansi, potensi terjadinya *double voting*, serta ketergantungan pada otoritas tunggal. Penelitian ini bertujuan untuk mengembangkan model sistem voting digital berbasis blockchain yang terdesentralisasi dengan mengintegrasikan mekanisme *Zero-Knowledge Proof* (ZKP) guna meningkatkan keamanan sekaligus menjaga privasi pemilih. Metode yang digunakan meliputi perancangan arsitektur sistem, pengembangan *smart contract*, serta implementasi dan pengujian sistem berbasis *Ethereum blockchain*. Model yang diusulkan diimplementasikan melalui sistem e-voting dengan memanfaatkan *smart contract* berbasis Solidity 0.8.19, framework Hardhat, serta arsitektur *hybrid* yang mengombinasikan backend API (Express.js dan MySQL) dengan jaringan *blockchain* publik. Hasil penelitian menunjukkan bahwa sistem mampu menjamin integritas data melalui sifat *immutability* blockchain, mencegah kecurangan seperti *double voting*, serta memungkinkan verifikasi publik tanpa mengungkap identitas pemilih melalui penerapan ZKP. Dengan demikian, model yang dikembangkan dapat menjadi solusi alternatif dalam membangun sistem voting digital yang transparan, aman, dan terpercaya.

Kata kunci: e-voting, blockchain, zero-knowledge proof, smart contract, desentralisasi, keamanan informasi.

A. Pendahuluan

Proses pemungutan suara (*voting*) merupakan pilar fundamental dalam sistem demokrasi yang berfungsi sebagai mekanisme utama dalam menentukan arah kebijakan dan kepemimpinan suatu negara. Keberhasilan suatu sistem pemilihan sangat ditentukan oleh tingkat kepercayaan publik terhadap integritas, transparansi, dan akuntabilitas proses yang berlangsung. Namun demikian, sistem voting konvensional—baik berbasis kertas maupun sistem digital terpusat—masih menghadapi berbagai tantangan serius, seperti potensi manipulasi data, kurangnya transparansi, risiko terjadinya *double voting*, serta ketergantungan pada otoritas tunggal yang dapat menimbulkan konflik kepentingan dan *single point of failure* [1].

Seiring dengan perkembangan teknologi informasi, berbagai pendekatan telah diusulkan untuk meningkatkan keamanan dan transparansi sistem voting, salah satunya melalui pemanfaatan teknologi blockchain. Blockchain memiliki karakteristik utama berupa desentralisasi, *immutability*, serta transparansi berbasis kriptografi yang memungkinkan pencatatan data secara permanen dan tidak dapat diubah. Dalam konteks sistem voting, setiap suara yang diberikan akan tersimpan dalam *distributed ledger* yang dapat diverifikasi secara publik tanpa memerlukan pihak ketiga yang dipercaya (*trusted third party*). Hal ini menjadikan

blockchain sebagai solusi potensial dalam membangun sistem pemilihan yang lebih aman dan transparan [2].

Meskipun demikian, penerapan blockchain dalam sistem voting tidak terlepas dari tantangan, khususnya terkait dengan aspek privasi pemilih. Transparansi tinggi yang ditawarkan oleh blockchain berpotensi membuka informasi sensitif apabila tidak diimbangi dengan mekanisme perlindungan data yang memadai. Oleh karena itu, diperlukan pendekatan kriptografi lanjutan yang mampu menjaga kerahasiaan identitas pemilih tanpa mengurangi kemampuan sistem dalam melakukan verifikasi. Salah satu pendekatan yang relevan adalah *Zero-Knowledge Proof* (ZKP), yaitu metode kriptografi yang memungkinkan pembuktian suatu informasi tanpa mengungkapkan informasi tersebut secara langsung. Integrasi ZKP dalam sistem voting berbasis blockchain memungkinkan terciptanya sistem yang tidak hanya transparan dan aman, tetapi juga menjaga anonimitas pemilih secara optimal [3].

Penelitian ini mengusulkan suatu model sistem voting digital berbasis blockchain yang mengintegrasikan mekanisme *Zero-Knowledge Proof* untuk menghasilkan sistem pemilihan yang transparan, aman, dan terdesentralisasi. Model yang dikembangkan diimplementasikan dalam aplikasi voting sebagai bentuk validasi konseptual dan teknis. Sistem ini dibangun menggunakan platform Ethereum, dengan *smart contract* berbasis Solidity versi 0.8.19 dan framework Hardhat sebagai lingkungan pengembangan dan pengujian. Selain itu, arsitektur sistem dirancang secara *hybrid* dengan mengombinasikan penyimpanan lokal, backend API berbasis Express.js dan MySQL, serta integrasi opsional dengan jaringan blockchain publik guna meningkatkan fleksibilitas, skalabilitas, dan efisiensi sistem.

Melalui pendekatan tersebut, penelitian ini diharapkan mampu memberikan kontribusi dalam pengembangan sistem e-voting yang lebih andal dengan mengatasi berbagai kelemahan sistem konvensional. Integrasi blockchain dan *Zero-Knowledge Proof* menjadi inovasi utama dalam penelitian ini, yang tidak hanya menjamin keamanan dan transparansi, tetapi juga menjaga privasi pemilih secara komprehensif. Dengan demikian, model yang diusulkan berpotensi menjadi referensi dalam implementasi sistem voting digital yang terpercaya di masa depan, baik pada skala institusi maupun nasional.

B. Metode

1) Pendekatan Penelitian

Penelitian ini menggunakan pendekatan analisis deskriptif-eksplanatif dengan metode studi kasus terhadap repositori votingApp_web3. Analisis dilakukan secara komprehensif terhadap kode sumber, dokumentasi teknis, dan arsitektur sistem yang tersedia di GitHub, didukung oleh pengujian langsung pada lingkungan lokal (localhost:8080).

2) Alat dan Teknologi Analisis

Komponen	Teknologi	Versi	Fungsi
Smart Contract Dev	Hardhat	2.17.0	Kompilasi, deployment, testing
Smart Contract Lang	Solidity	0.8.19	Bahasa smart contract
Web3 Library	Web3.js	4.1.2	Interaksi blockchain dari frontend
Blockchain Library	Ethers.js	6.7.0	Interaksi blockchain dari backend
Wallet Integration	MetaMask	Latest	Autentikasi pengguna
Backend Framework	Express.js	Latest	REST API server
Database	MySQL	5.7+	Penyimpanan data persisten
Frontend	HTML5/CSS3/JS	ES6+	Antarmuka pengguna modular

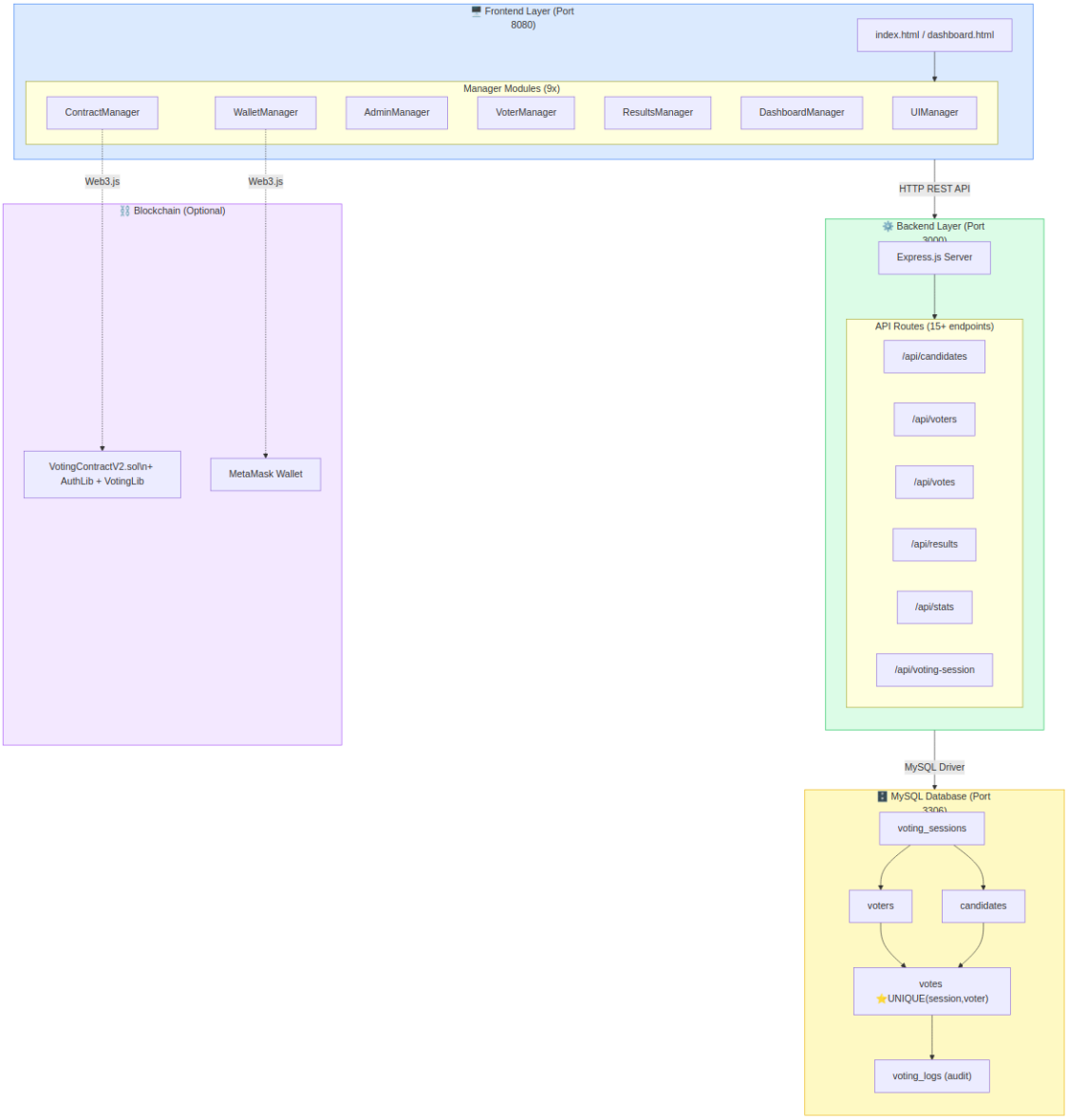
3) Tahapan Analisis

- Tahap 1 — Studi Dokumentasi: Membaca seluruh dokumentasi teknis (README.md, SETUP_GUIDE.md, API_REFERENCE.md, SECURITY_ANALYSIS.md, DEPLOYMENT_GUIDE.md, dan seluruh file di folder docs/diagrams).
- Tahap 2 — Analisis Arsitektur: Memetakan komponen dan hubungan antar-lapisan (blockchain layer, backend layer, frontend layer, database layer).
- Tahap 3 — Review Smart Contract: Menganalisis logika bisnis, mekanisme keamanan (modifier, mapping, event), dan pola enkripsi.
- Tahap 4 — Pengujian Langsung: Menjalankan sistem pada lingkungan lokal dan mendokumentasikan hasil melalui screenshot.
- Tahap 5 — Evaluasi Keamanan: Menilai mekanisme anti-double voting, access control, input validation, dan state management.
- Tahap 6 — Sintesis dan Pelaporan: Menyusun temuan analisis secara sistematis dan memberikan rekomendasi pengembangan.

4) Implementasi

a) Arsitektur Sistem

Sistem e-voting mengimplementasikan arsitektur *hybrid* empat-lapisan yang menggabungkan penyimpanan lokal, backend API, dan blockchain opsional. Arsitektur ini dirancang untuk memberikan fleksibilitas penggunaan, mulai dari mode demo berbasis localStorage hingga deployment penuh dengan blockchain testnet.

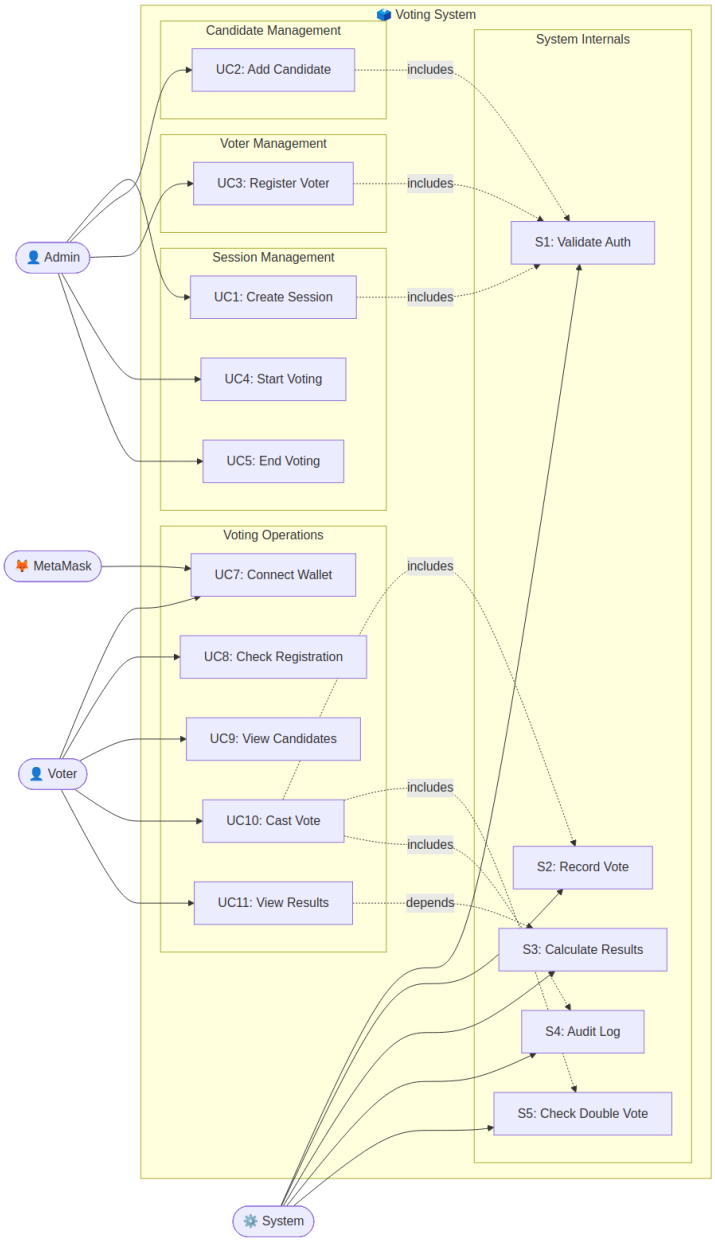


Gambar 1. Diagram Komponen Arsitektur Hybrid e-voting

Layer	Komponen	Teknologi	Deskripsi
Blockchain	VotingContractV2 + Libraries	Solidity/Ethereum	Logika voting immutable di blockchain
Frontend	9 Manager Modules	HTML5/CSS3/JS	UI modular dengan tab Admin/Voter/Results
Backend API	Express.js Server	Node.js/Express	15+ REST endpoints (port 3000)
Database	db_voting	MySQL 5.7+	8 tabel + 2 view + 2 stored procedure

b) *Use Case* Diagram

Diagram *use case* menggambarkan seluruh interaksi yang dapat dilakukan oleh aktor-aktor utama: Admin (mengelola sesi, kandidat, dan pemilih), Voter (menghubungkan wallet, melihat kandidat, memberikan suara), MetaMask (menyediakan autentikasi wallet), dan System (validasi, pencatatan, kalkulasi).



Gambar 2. Use Case Diagram Sistem Voting Digital

c) Smart Contract

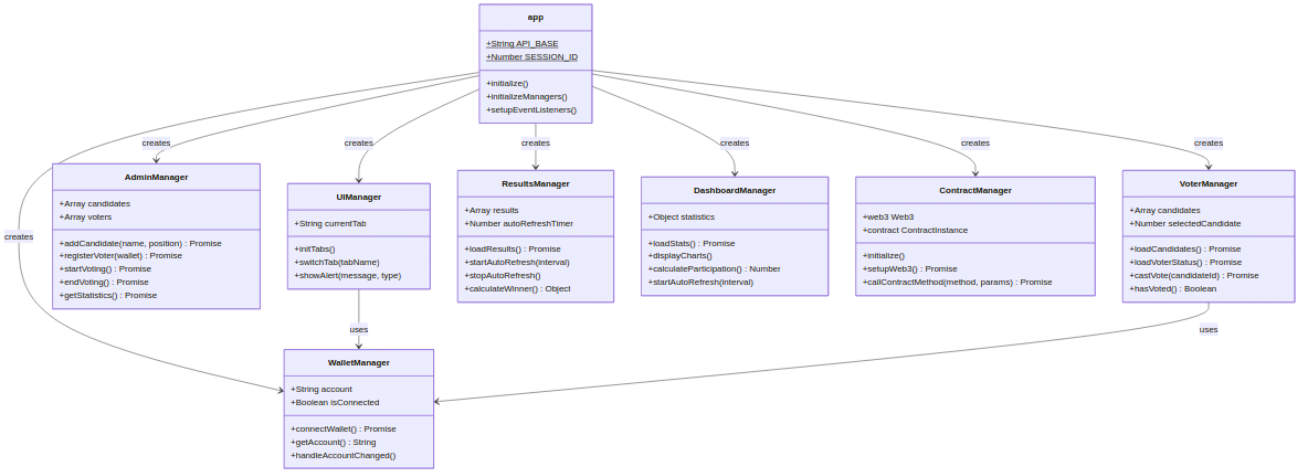
Implementasi *smart contract* menggunakan pola *library* yang memisahkan logika bisnis ke dalam modul-modul yang dapat diuji secara independen. Total ~650 LOC yang terdiri dari VotingContractV2.sol (~200 LOC) sebagai kontrak utama, ditambah AuthLib.sol dan VotingLib.sol sebagai library pendukung.

Event yang di-emit smart contract untuk audit trail meliputi: VoterRegistered, VoteCasted, VotingStarted, VotingEnded, CandidateAdded, dan VotersReset. Setiap event menyertakan indexed address dan timestamp untuk kemudahan pelacakan *on-chain.*

d) Frontend Modular — Class Diagram

Frontend dibangun menggunakan sembilan modul JavaScript independen yang masing-masing bertanggung jawab atas domain fungsional yang spesifik. Pendekatan ini menggunakan

pola *Singleton* (setiap manager diinstansiasi sekali) dan Observer Pattern untuk event handling.

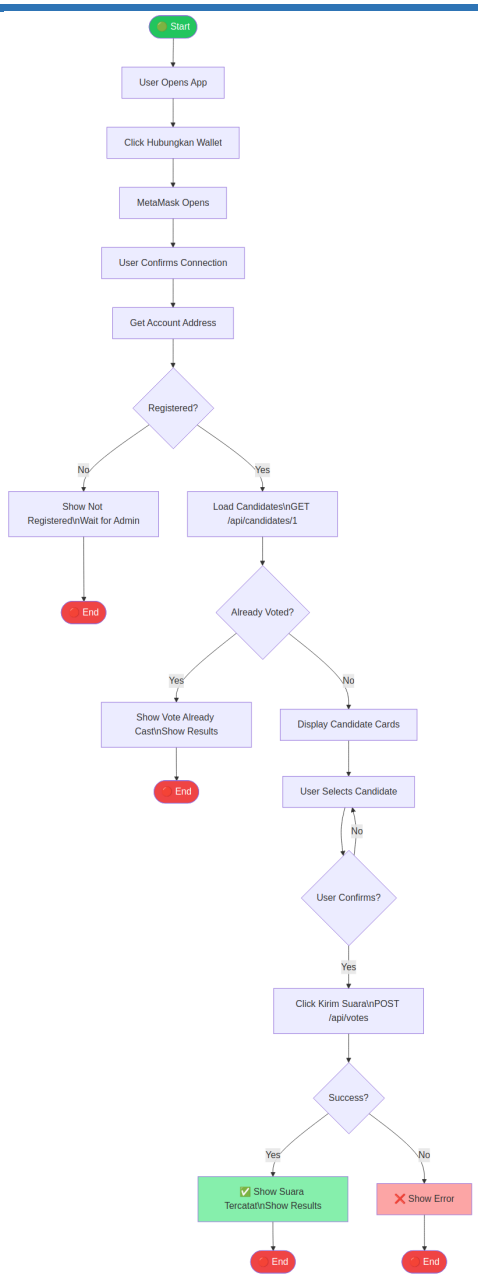


Gambar 3. Class Diagram Frontend Manager Modules

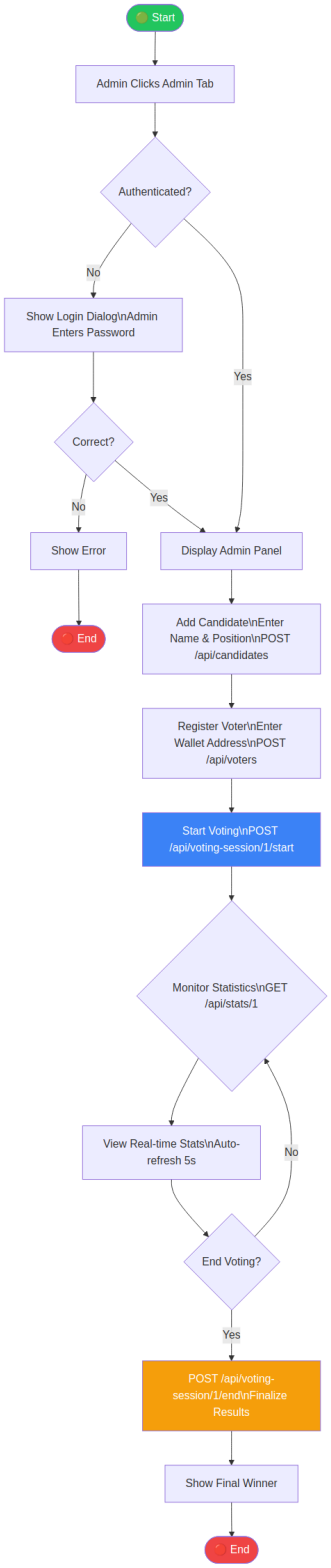
Modul	Fungsi Utama	Refresh
WalletManager	Koneksi MetaMask, manajemen akun Web3	—
ContractManager	Interaksi smart contract via Web3.js	—
AdminManager	Tambah kandidat, daftar pemilih, kontrol sesi	—
VoterManager	Cast vote, cek status, verifikasi registrasi	—
ResultsManager	Tampilan hasil real-time	5 detik
DashboardManager	Analytics real-time, statistik voting	3 detik
UIManager	Navigasi tab, state UI, notifikasi	—
LocalDataManager	Manajemen localStorage sebagai primary storage	—
app.js	Inisialisasi aplikasi & koordinasi modul	—

e) Alur Kerja Sistem

Diagram di bawah ini menggambarkan alur lengkap dari perspektif pemilih dan admin:



Gambar 4. Activity Diagram: Alur Voting Pemilih



Gambar 5. Activity Diagram: Alur Operasi Admin

f) Deployment

Sistem mendukung deployment ke beberapa jaringan blockchain melalui Hardhat. Proses kompilasi menghasilkan ABI dan *bytecode* di direktori build/artifacts/, sementara informasi deployment (alamat kontrak, network) disimpan di deployments/ sebagai file JSON untuk

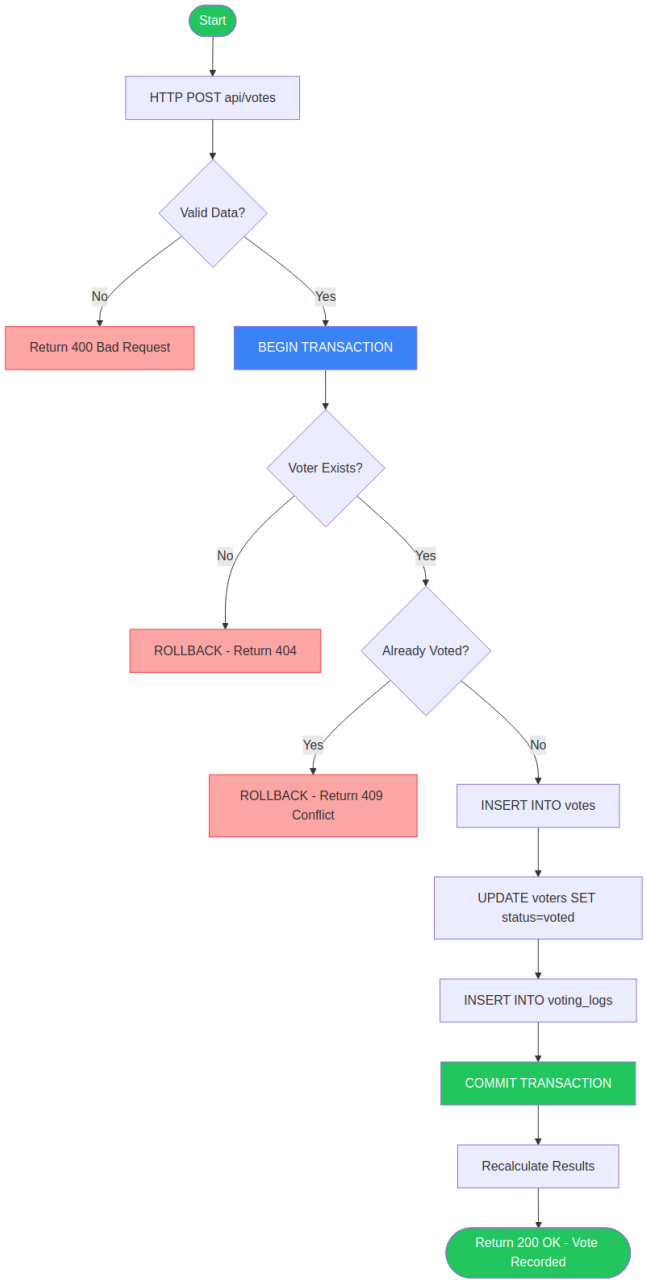
referensi frontend.

Jaringan	Chain ID	Mata Uang	RPC Provider	Keterangan
Sepolia	11155111	ETH	Infura/Alchemy	Rekomendasi utama
Polygon Mumbai	80001	MATIC	MaticVigil	Biaya lebih rendah
Polygon Amoy	80002	MATIC	MaticVigil	Testnet terbaru
Hardhat Local	31337	ETH	localhost:8545	Development

C. Hasil dan Pembahasan

1) Mekanisme ACID Transaction pada Vote Recording

Alur berikut mengilustrasikan mekanisme ACID transaction database yang merupakan inti sistem keamanan *anti-double voting*. Setiap operasi INSERT vote dilindungi oleh transaction lock, validasi bertingkat, dan UNIQUE constraint:

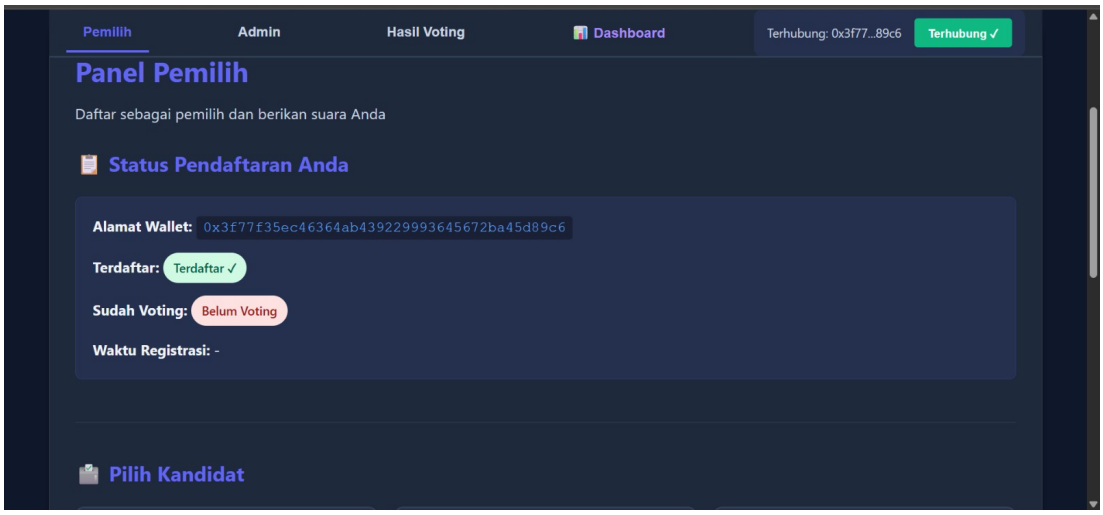


Gambar 6. Alur Transaksi Database ACID pada Pencatatan Suara

2) Hasil Pengembangan

a) Panel Pemilih — Status Pendaftaran

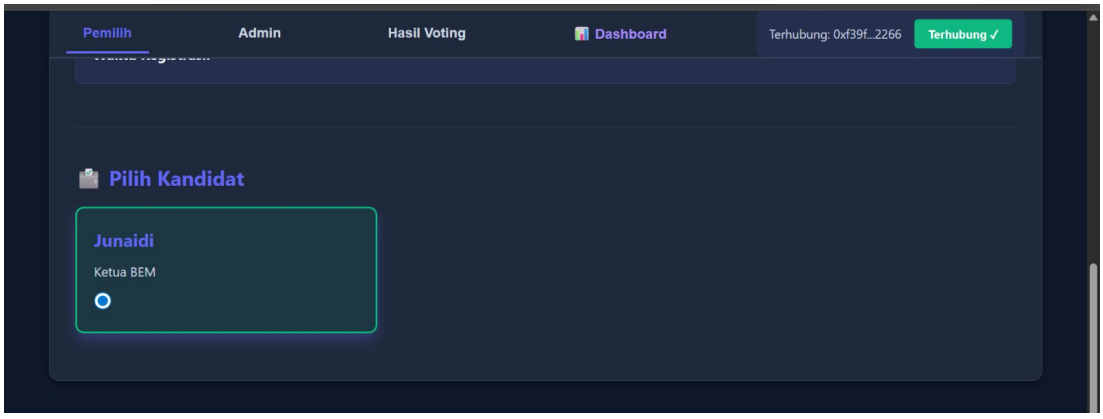
Gambar berikut menunjukkan tampilan Panel Pemilih setelah wallet MetaMask berhasil terhubung. Sistem berhasil mengidentifikasi alamat wallet pemilih (0x3f77f35ec46364ab439229993645672ba45d89c6), menampilkan status terdaftar dengan badge hijau (Terdaftar ✓), dan status voting (Belum Voting) sebelum memberikan suara. Fitur ini memanfaatkan endpoint GET /api/voters/{session}/{wallet} secara real-time.



Gambar 7. Tampilan Panel Pemilih: Status Pendaftaran & Koneksi Wallet MetaMask

b) Antarmuka Pemilihan Kandidat

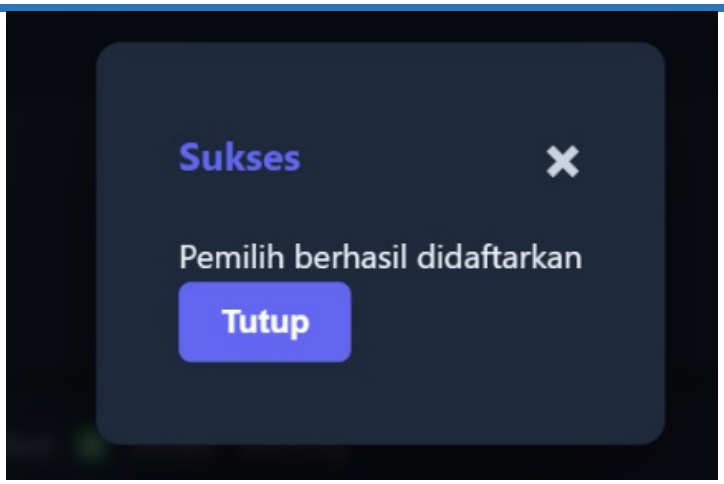
Tampilan daftar kandidat ditampilkan dalam format card yang responsif. Setiap card menampilkan nama kandidat, posisi yang diperebutkan, dan radio button untuk pemilihan. Pada pengujian ini, kandidat yang tersedia adalah Junaidi untuk posisi Ketua BEM. Card yang dipilih mendapatkan highlight border berwarna cyan sebagai visual feedback kepada pemilih.



Gambar 8. Tampilan Antarmuka Pilih Kandidat dengan Card Selection

c) Konfirmasi Registrasi Pemilih

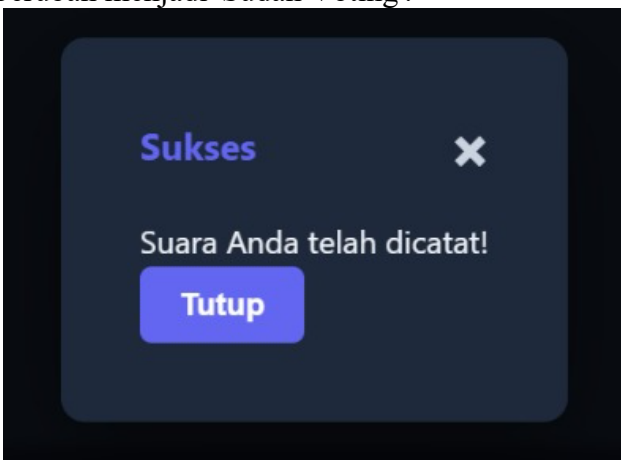
Modal dialog konfirmasi muncul setelah admin berhasil mendaftarkan pemilih baru. Pesan 'Pemilih berhasil didaftarkan' mengkonfirmasi bahwa alamat wallet telah berhasil diinsert ke tabel voters di database MySQL dengan status 'registered'. Di background terlihat daftar pemilih terdaftar yang telah ter-update secara otomatis.



Gambar 9. Modal Konfirmasi: Registrasi Pemilih Berhasil

d) Konfirmasi Pengiriman Suara

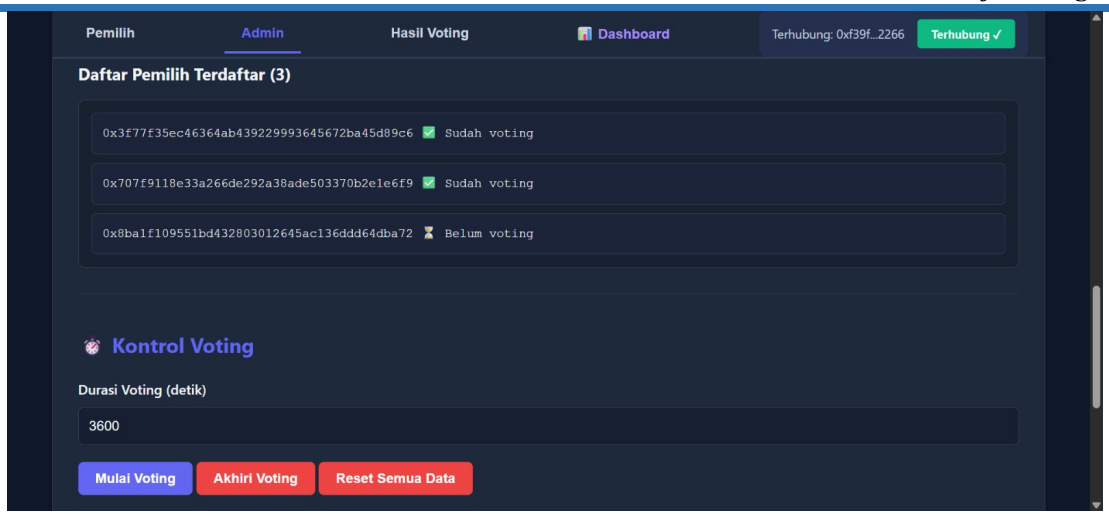
Modal dialog konfirmasi 'Suara Anda telah dicatat!' muncul setelah pemilih berhasil mengirimkan suara. Pada tahap ini, sistem telah menyelesaikan seluruh rangkaian ACID transaction: verifikasi pemilih, pengecekan status voting, INSERT ke tabel votes, UPDATE status voter menjadi 'voted', dan INSERT ke voting_logs sebagai audit trail. Status pemilih di panel secara otomatis berubah menjadi 'Sudah Voting'.



Gambar 10. Modal Konfirmasi: Suara Berhasil Dicatat

e) Panel Admin — Daftar Pemilih & Kontrol Voting

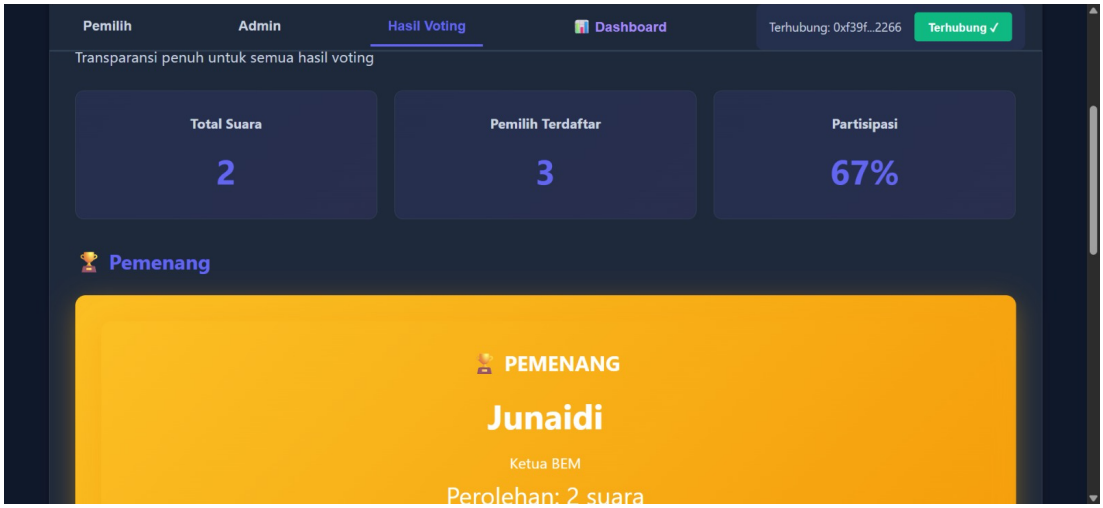
Tampilan panel admin menunjukkan daftar 3 pemilih terdaftar dengan status voting real-time: dua pemilih telah memberikan suara (Sudah voting ✓) dan satu pemilih belum (Belum voting ⏳). Panel Kontrol Voting menampilkan durasi sesi (3600 detik = 1 jam) beserta tiga tombol aksi utama: Mulai Voting (biru), Akhiri Voting (merah), dan Reset Semua Data (merah). Fitur ini memvalidasi implementasi role-based access control yang membatasi kontrol sesi hanya untuk admin.



Gambar 11. Panel Admin: Daftar Pemilih Terdaftar & Kontrol Voting Session

f) Halaman Hasil Voting — Tampilan Pemenang

Halaman Hasil Voting menampilkan rekap komprehensif dengan tiga statistik utama: Total Suara (2), Pemilih Terdaftar (3), dan tingkat Partisipasi (67%). Sistem secara otomatis mengidentifikasi dan menampilkan pemenang dalam banner berwarna kuning yang mencolok — dalam pengujian ini, Junaidi (Ketua BEM) menang dengan perolehan 2 suara. Data diperbarui secara otomatis setiap 5 detik melalui mekanisme auto-refresh ResultsManager, memastikan transparansi penuh selama proses voting berlangsung.



Gambar 12. Halaman Hasil Voting: Statistik Real-time & Banner Pemenang

D. Simpulan

Sistem Voting Digital Berbasis Blockchain dengan Zero-Knowledge Proof Untuk Pemilihan Yang Transparan dan Terdesentraliasi merupakan implementasi sistem voting digital berbasis blockchain yang komprehensif dan telah teruji. Berdasarkan pengujian langsung yang terdokumentasi dalam laporan ini (Gambar 5.7 hingga 5.12), sistem berhasil mendemonstrasikan seluruh alur fungsional utama: koneksi wallet MetaMask, registrasi pemilih oleh admin, pemilihan kandidat, pengiriman suara dengan ACID transaction, tracking status real-time, dan tampilan hasil voting dengan kalkulasi partisipasi otomatis.

Capaian teknis yang menonjol: (1) Arsitektur hybrid modular 4-layer dengan 9 manager module frontend; (2) Mekanisme anti-double voting berlapis tiga yang terbukti efektif; (3)

ACID transaction database dengan UNIQUE constraint sebagai last-line of defense; (4) Dukungan multi-testnet blockchain; serta (5) UI responsif dengan auto-refresh 5 detik untuk transparansi real-time. Keterbatasan utama: manajemen private key via .env, belum ada audit smart contract formal, dan potensi inkonsistensi sinkronisasi tiga sumber data.

Daftar Pustaka

[1] T. &. N. M. Hidayat, "Evaluasi Sistem Voting Elektronik Terpusat dan Tantangannya di Indonesia," *Jurnal Nasional Teknologi dan Sistem Informasi,* vol. 9, no. 1, p. 15–23, 2023.

[2] D. P. B. &. F. R. Wijaya, "Desain Sistem E-Voting Terdesentralisasi Berbasis Blockchain Ethereum," *Jurnal Ilmiah Komputer dan Informatika,* vol. 13, no. 1, p. 101–110, 2024.

[3] N. &. K. A. Putri, "Integrasi Zero-Knowledge Proof dalam Sistem Voting Digital untuk Menjaga Anonimitas Pemilih," *Jurnal Teknologi dan Sistem Komputer,* vol. 13, no. 2, p. 89–98, 2025.