Jurnal Minfo Polgan
Volume 14, Nomor 2, November 2025
DOI : https://doi.org/10.33395/jmp.v14i2.15536
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Sistem E-Voting berbasis Blockchain dengan Autentikasi Biometrik Sidik Jari dan Protokol Zero-Knowledge Proof Untuk Pengaman Privasi

[1]Muhammad Riswanto, [2]Lindawati, [3]Nurhajar Anugraha, [4]Asrul
[1,2,3]Politeknik Negeri Sriwijaya, Palembang, Indonesia
[4]Universitas Halu Oleo Kendari, Indonesia
[1]muhammadriswantosenpai@gmail.com, [2]nurhajar.anugraha@polsri.ac.id,
[3]lindawati@polsri.ac.id, [4]asrul@akba.ac.id

Submit : 26 Okt 25 | **Diterima** : 03 Nov 2025 | **Terbit** : 05 Nov 2025

ABSTRAK

Penelitian ini bertujuan untuk mengembangkan sistem e-voting berbasis blockchain dengan autentikasi biometrik sidik jari serta penerapan protokol zero-knowledge proofs sebagai pengamanan tambahan terhadap data pemilih dan hasil suara. Permasalahan utama yang dihadapi dalam sistem pemungutan suara elektronik konvensional adalah rendahnya kepercayaan terhadap keamanan data dan potensi manipulasi hasil. Metode penelitian yang digunakan mencakup perancangan sistem dengan arsitektur client-server, implementasi teknologi blockchain untuk pencatatan suara yang terenkripsi, serta integrasi biometrik sidik jari menggunakan BiometricPrompt API pada Android. Selain itu, sistem diverifikasi dengan kode OTP melalui email institusional sebagai bentuk validasi ganda pengguna. Hasil pengujian menunjukkan bahwa sistem dapat berjalan dengan baik dan memberikan keamanan yang tinggi karena setiap data suara tersimpan secara permanen dan tidak dapat diubah di jaringan blockchain. Autentikasi biometrik juga memastikan bahwa setiap pemilih terverifikasi secara unik sehingga tidak terjadi pemungutan suara ganda. Dengan demikian, sistem e-voting ini dinilai layak diterapkan untuk lingkungan akademik dan dapat dikembangkan lebih lanjut untuk pemilihan umum berskala lebih besar.

Kata Kunci: e-voting; blockchain; biometrik; zero-knowledge proof; keamanan data

PENDAHULUAN

Pemungutan suara yang aman, transparan, dan bisa dipercaya adalah pondasi utama dalam pengambilan keputusan bersama. Sayangnya, sistem pemilihan tradisional, entah yang pakai kertas atau mesin elektronik yang terpusat, sering menghadapi masalah yang menimbulkan keraguan. Cara manual rentang terjadi kesalahan karena faktor manusia atau bahkan dapat di curangi, sementara *e-voting* yang terpusat rentan diserang *hacker*, seperti manipulasi data, pembobolan *server*, atau serangan yang bikin sistem mati total. Meski *e-voting* lebih efisien dan mudah diakses, sifatnya yang bergantung pada satu pusat kontrol menciptakan risiko besar, di mana satu kesalahan bisa merusak semuanya. Untuk menjaga integritas demokrasi, kita butuh jaminan lebih diantaranya suara dihitung tepat dan identitas pemilih tetap terjamin kerahasiaannya.

Teknologi *blockchain* datang sebagai solusi menarik untuk atasi kelemahan sistem terpusat tersebut. Dengan menyebarkan catatan suara ke banyak *node* di jaringan, *blockchain* menciptakan rekam jejak transaksi yang permanen dan terbuka. Setiap suara disimpan sebagai blok yang terhubung lewat kriptografi, jadi hampir mustahil diubah atau dihapus tanpa ketahuan seluruh jaringan. Pendekatan desentralisasi ini menghapus ketergantungan pada satu pihak berkuasa, sehingga sistem lebih tahan terhadap kecurangan atau penyensoran. Akhirnya, *blockchain* bisa jadi fondasi kuat untuk *e-voting* yang lebih

Jurnal Minfo Polgan
Volume 14, Nomor 2, November 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15536 p-ISSN : 2089-9424

jujur dan sulit dimanipulasi.

Tapi, keterbukaan *blockchain* yang total justru menimbulkan masalah privasi. Jika tidak dirancang hati-hati, semua catatan suara, bahkan identitas pemilih dapat dilihat siapa saja. Untuk mengatasi permasalahan tersebut dibutuhkan teknik kriptografi seperti *Zero-Knowledge Proof* (ZKP) yang menjadi kunci untuk menyeimbangkan transparansi dan privasi. ZKP memungkinkan pembuktian sesuatu benar atau tidak, misalnya bahwa pemilih sudah terdaftar dan belum menggunakan hak suaranya, tanpa mengungkap informasi lain selain fakta itu sendiri. Lewat cara ini, *e-voting* dapat menverifikasi suara dan status pemilih tanpa mengorbankan anonimitas pemilih. Selain privasi, keamanan akses juga penting, autentikasi biometrik seperti sidik jari memberikan verifikasi identitas yang handal, karena setiap sidik jari unik dan susah dipalsukan. Di era saat ini, penggunaan sidik jadi sudah menjadi hal biasa apalagi saat ini kebanyakan ponsel pintar telah memiliki sistem pemindai sidik jari yang aman, jadi hanya pemilih asli yang dapat masuk login ke sistem sesuai dengan data sidik jari yang telah terdaftarkan.

Xue dkk.(2023) membuat sistem *e-voting* berbasis *blockchain* dengan metode *anonymously convertible ballots* (CLS) untuk melindungi anonimitas pemilih. Sistem yang dibangun secara efisien dan menghindari pembuktian kriptografi yang rumit, akan tetapi kelamahan sistemnya terletak pada privasi yang bergantung pada skema CLS itu dan tidak bahas soal kemudahan penggunaan seperti biaya transaksi di *blockchain*.

Pada penelitian ini, penggabung teknologi *blockchain* untuk menjaga integritas data, Protokol ZKP untuk merahasiakan suara, dan biometrik sidik jari untuk autentikasi, maka dirancanglah kerangka *e-voting* yang memenuhi kebutuhan keamanan dan privasi sekaligus.

TINJAUAN PUSTAKA

Pemungutan Suara Elektronik (*E-Voting*)

E-voting merujuk pada penggunaan perangkat elektronik dalam satu atau lebih tahapan proses pemungutan suara, yang mencakup pendaftaran pemilih, pemberian suara, serta penghitungan hasil. Secara umum, sistem ini dapat dibedakan menjadi dua bentuk utama: *Direct Recording Electronic* (DRE), di mana suara direkam langsung pada perangkat di tempat pemungutan suara (TPS), dan *remote internet voting*, yang memungkinkan pemilih untuk memberikan suara dari lokasi mana pun. Sistem yang dikembangkan dalam penelitian ini termasuk dalam kategori kedua, karena menyediakan fleksibilitas dan akses yang lebih luas bagi pemilih.

Agar dapat diandalkan, sistem *e-voting* harus memenuhi prinsip-prinsip inti, yaitu keamanan dan integritas (yang mencakup ketahanan terhadap serangan dan manipulasi), transparansi serta kemampuan audit, privasi atau anonimitas (untuk menjaga kerahasiaan pilihan pemilih), *verifiability* (di mana pemilih dapat memeriksa suara mereka sendiri dan publik dapat memverifikasi hasil secara keseluruhan), serta aksesibilitas dan akurasi bagi seluruh pemilih yang sah. Namun, tantangan utama terletak pada kenyataan bahwa banyak sistem terpusat masih bergantung pada server pusat, sehingga rentan menjadi target serangan. Selain itu, menyeimbangkan antara keterbukaan proses pemungutan suara dengan perlindungan kerahasiaan pemilih tetap merupakan tugas kriptografi yang kompleks.

Blockchain dan Smart Contract

Blockchain menyajikan pendekatan inovatif untuk mengatasi kelemahan sistem terpusat. Pencatatan suara didistribusikan ke berbagai node dan dihubungkan secara

Jurnal Minfo Polgan
Volume 14, Nomor 2, November 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15536 p-ISSN : 2089-9424

berantai, sehingga menciptakan jejak transaksi yang bersifat *immutable* dan sulit dimodifikasi tanpa terdeteksi. Dengan demikian, ketergantungan pada satu entitas pengendali data dapat diminimalisir, sehingga mengurangi risiko titik kegagalan tunggal dan meningkatkan ketahanan terhadap upaya sensor.

Selain itu, *smart contract*, seperti yang ditemukan pada *platform Ethereum*, berfungsi sebagai mekanisme otomatis dan transparan untuk mengatur berbagai tahapan pemilihan, termasuk pendaftaran pemilih, periode pemungutan suara, serta penghitungan hasil. Beberapa pendekatan juga mengintegrasikan *blockchain* dengan teknik *Zero-Knowledge Proofs* guna menambahkan lapisan privasi tanpa mengorbankan kapabilitas verifikasi. Dalam penelitian ini, pengembangan dan pengujian sistem dilakukan pada *Sepolia testnet*, yaitu lingkungan uji publik yang menyerupai jaringan utama, untuk memastikan keamanan dan efisiensi biaya. Selain itu, beberapa desain mengeksplorasi penggunaan pembangkitan bilangan acak yang terdesentralisasi demi menjamin keadilan proses.

Autentikasi Biometrik pada *Platform Android*

Autentikasi yang kuat memastikan bahwa hanya pemilih yang sah saja yang dapat menggunakan hak suaranya. Biometrik sidik jari menonjol karena sifatnya yang unik dan sulit dipalsukan, sehingga sangat sesuai sebagai mekanisme akses ke sistem *e-voting*. Pada *platform Android*, ekosistem keamanan *modern*, melalui *Android Keystore* dan *BiometricPrompt*, membantu melindungi kunci kriptografi dalam lingkungan yang didukung perangkat keras serta menghadirkan dialog autentikasi yang dikelola oleh sistem. Pendekatan ini mengurangi risiko peniruan antarmuka dan mengikat penggunaan kunci pada keberhasilan autentikasi, sehingga meningkatkan jaminan atas kehadiran dan keabsahan pengguna tanpa perlu mengungkapkan data sensitif kepada aplikasi.

Zero-Knowledge Proof dan Protokol *Semaphore*

Zero-Knowledge Proof (ZKP) memungkinkan seseorang untuk membuktikan kebenaran suatu klaim, seperti status pendaftaran pemilih dan belum adanya penggunaan hak suara, tanpa mengungkapkan informasi tambahan di luar klaim tersebut. Dengan demikian, proses verifikasi dapat berlangsung secara efektif sekaligus menjaga anonimitas pemilih. Dalam konteks *blockchain*, keluarga ZK-SNARKs sering digunakan karena ukuran bukti yang ringkas serta kecepatan verifikasi yang tinggi.

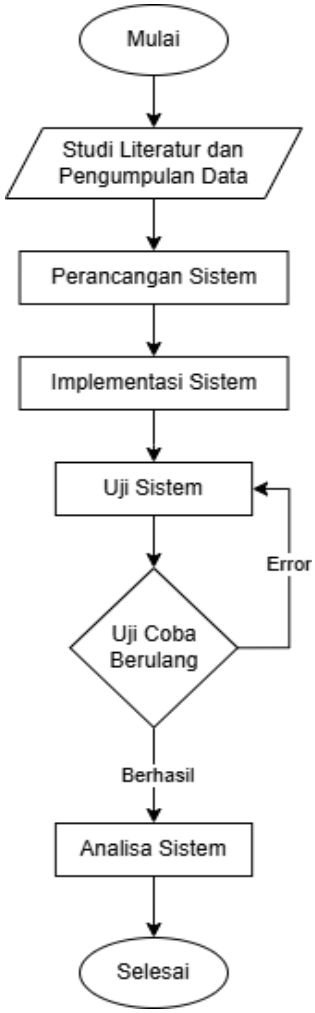
Semaphore merupakan kerangka ZKP yang memungkinkan pengguna untuk mengirimkan "sinyal", seperti suara dalam pemungutan suara, secara anonim, sambil mencegah duplikasi melalui mekanisme *nullifier*. Pendekatan ini memastikan bahwa setiap individu hanya dapat memberikan satu suara, tanpa kemungkinan pelacakan kembali ke identitas asli. Beberapa implementasi memerlukan trusted setup untuk menghasilkan parameter publik, di mana keamanannya bergantung pada asumsi bahwa setidaknya satu peserta yang jujur akan menghancurkan "*toxic waste*" yang terlibat dalam proses tersebut.

METODE PENELITIAN

Kerangka Penelitian

Penelitian ini dilakukan melalui serangkaian tahapan terstruktur yang dirancang untuk merancang, membangun, dan menguji sistem *e-voting* berbasis *blockchain* dengan fitur autentikasi biometrik dan *Zero-Knowledge Proofs* (ZKP). Blok diagram kerangka penelitian dapat dilihat pada gambar 1 sebagai berikut;

Jurnal Minfo Polgan
Volume 14, Nomor 2, November 2025
DOI : https://doi.org/10.33395/jmp.v14i2.15536
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 1 Blok Diagram Kerangka Penelitian

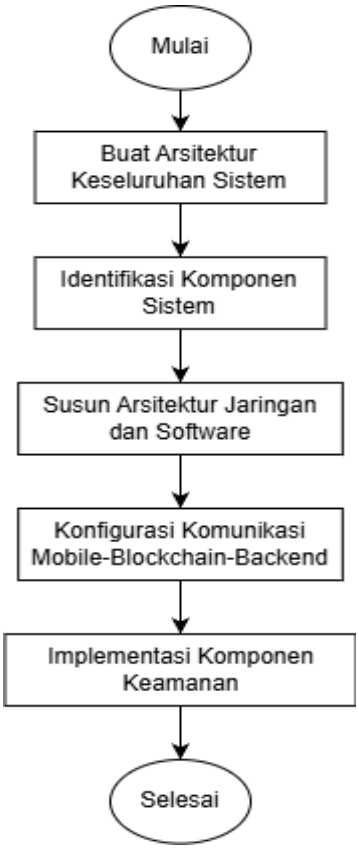
1. Mulai
2. Studi Literatur
   Pengumpulan pengetahuan dari jurnal, buku, dan dokumentasi teknis terkait *e-voting*, *blockchain*, *smart contract*, ZKP, dan biometrik, lalu penyusunan kebutuhan fungsional serta non-fungsional sistem.
3. Perancangan Sistem
   Penyusunan alur kerja dari registrasi hingga pemungutan dan penghitungan suara, perancangan komponen utama (klien, layanan, dan buku besar terdistribusi), antarmuka pengguna, model data, serta pola interaksi antarkomponen.
4. Implementasi Bertahap
   Pembangunan komponen inti berdasarkan rancangan: logika on-chain, aplikasi pemilih di perangkat bergerak, layanan backend, serta dasbor administrator. Pengerjaan dilakukan iteratif per modul dengan pengujian unit di setiap tahap.
5. Pengujian Terstruktur
   Pengujian fungsional dan integrasi untuk memastikan alur berjalan sesuai desain, diikuti uji skenario keberhasilan dan kegagalan guna menilai ketahanan sistem. Temuan digunakan untuk perbaikan hingga perilaku sistem stabil.
6. Analisis & Sintesis Hasil

Jurnal Minfo Polgan
Volume 14, Nomor 2, November 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15536 p-ISSN : 2089-9424

Pengolahan hasil uji untuk menilai ketercapaian tujuan, membahas kekuatan dan keterbatasan, serta menarik implikasi praktis maupun arah pengembangan berikutnya.

Perancangan Sistem

Perancangan sistem difokuskan pada arsitektur secara keseluruhan, dengan identifikasi komponen inti serta penetapan hubungan antar-komponen tersebut. Secara umum, sistem mencakup aplikasi pemilih berbasis *Android*, dasbor *web* untuk *administrator*, layanan *backend* yang mengorkestrasi data *off-chain*, serta *smart contract* pada *blockchain* sebagai mekanisme pencatatan suara yang transparan dan dapat diaudit. Prinsip keamanan diterapkan sejak tahap awal, termasuk perlindungan akses pemilih melalui biometrik, pemeliharaan kerahasiaan suara dengan pembuktian tanpa pengungkapan identitas, serta pemisahan data *on-chain* dan *off-chain* untuk mendukung efisiensi sekaligus akuntabilitas. Perancangan sistem penelitian dapat dilihat pada gambar 2 sebagai berikut;



Gambar 2 Perancangan Keseluruhan Sistem

Aplikasi pemilih pada *platform Android* berfungsi sebagai antarmuka utama bagi pemilih, memungkinkan registrasi dan pemberian suara secara nyaman dan aman. Aplikasi ini menyediakan proses pendaftaran yang sederhana, termasuk verifikasi melalui *email* dengan *one-time password* (OTP). Keamanan akses dijamin melalui autentikasi biometrik sidik jari, sehingga hanya pemilih yang sah yang dapat mengaksesnya. Selain itu, aplikasi ini mengelola kunci kriptografi yang terikat pada perangkat dan menjalankan proses pembuktian secara lokal, menjaga agar data sensitif tetap terlindungi di sisi pemilih.

Jurnal Minfo Polgan
Volume 14, Nomor 2, November 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15536 p-ISSN : 2089-9424

Aplikasi *administrator* berbasis *web* menyediakan dasbor bagi panitia untuk mengelola siklus pemungutan suara secara terpusat namun tetap transparan. Melalui dasbor ini, *administrator* dapat membuat dan mengonfigurasi acara pemilihan, mendaftarkan kandidat, serta memulai atau mengakhiri periode pemungutan suara. Fitur pemantauan partisipasi dan status pemungutan disajikan secara ringkas, sementara komunikasi dengan backend dilakukan melalui *application programming interface* (API) yang dirancang khusus untuk kebutuhan pengelolaan data dan audit.

Layanan *backend* berperan sebagai lapisan orkestrasi yang menghubungkan *aplikasi* pemilih, aplikasi *administrator*, dan *blockchain*. Layanan ini menyediakan representational *state transfer* (*REST*) API bagi klien pemilih dan *administrator*. Data operasional non-sensitif, seperti daftar kandidat dan detail acara, disimpan dalam basis data relasional. Selain itu, *backend* menangani verifikasi OTP serta penyusunan daftar keanggotaan pemilih sah, yang kemudian dirujuk oleh selama verifikasi suara tanpa mengekspos identitas pribadi.

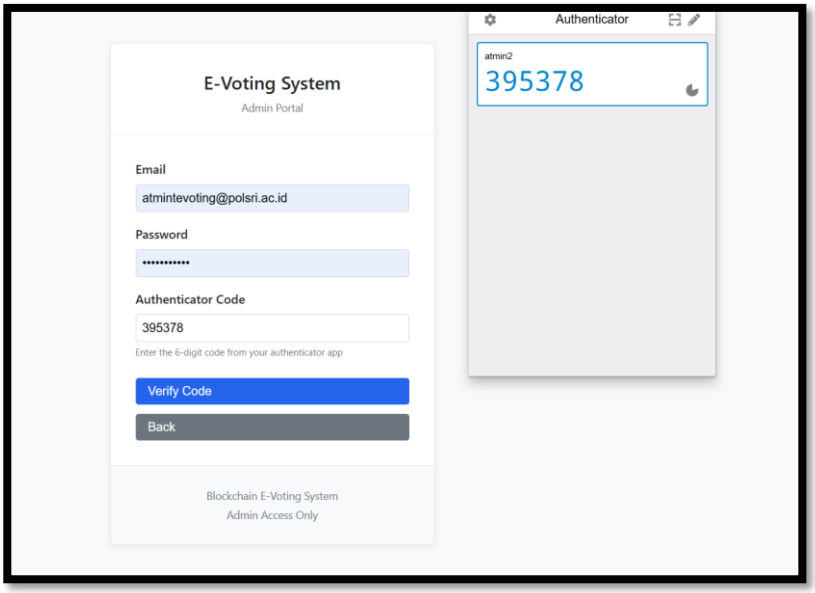
Smart contract pada *blockchain* menyediakan logika terdesentralisasi yang menjamin integritas proses secara keseluruhan. Kontrak ini memverifikasi bukti bahwa suara berasal dari pemilih sah tanpa mengungkap identitas, sekaligus mencegah pemungutan suara ganda. Pengelolaan status pemungutan suara, seperti pembukaan atau penutupan, serta pencatatan suara ke dalam perhitungan yang dapat diaudit secara publik, juga ditangani oleh kontrak ini. Operasionalnya dilakukan pada jaringan uji yang menyerupai lingkungan produksi, sehingga hasil dapat diverifikasi dengan risiko dan biaya yang lebih rendah.

HASIL DAN PEMBAHASAN

Halaman Login

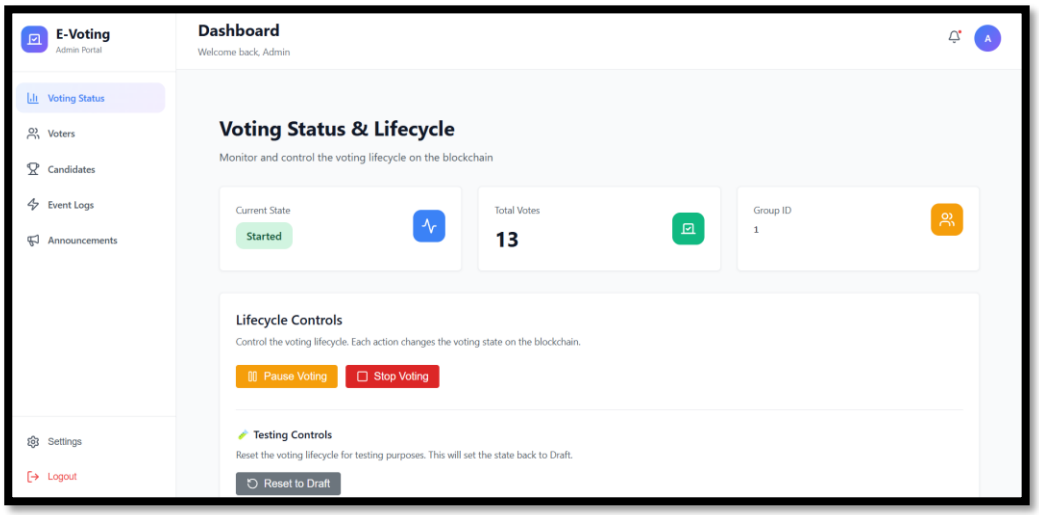
Halaman *login admin* dengan *display* TOTP (*Time-based One-Time Password*) adalah tampilan antarmuka masuk untuk *administrator* yang dilengkapi fitur autentikasi dua faktor (2FA). Dengan memasukkan *username*, *password*, dan kode TOTP yang dihasilkan secara sementara oleh aplikasi seperti *Google Authenticator* untuk meningkatkan keamanan. Kode ini berubah setiap 30 detik dan ditampilkan di app pengguna, bukan langsung di halaman web, untuk mencegah akses tidak sah seperti dapat dilihat pada gambar 3

Jurnal Minfo Polgan
Volume 14, Nomor 2, November 2025
DOI : https://doi.org/10.33395/jmp.v14i2.15536
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 3 Halaman *Login Admin* dan *input* TOTP

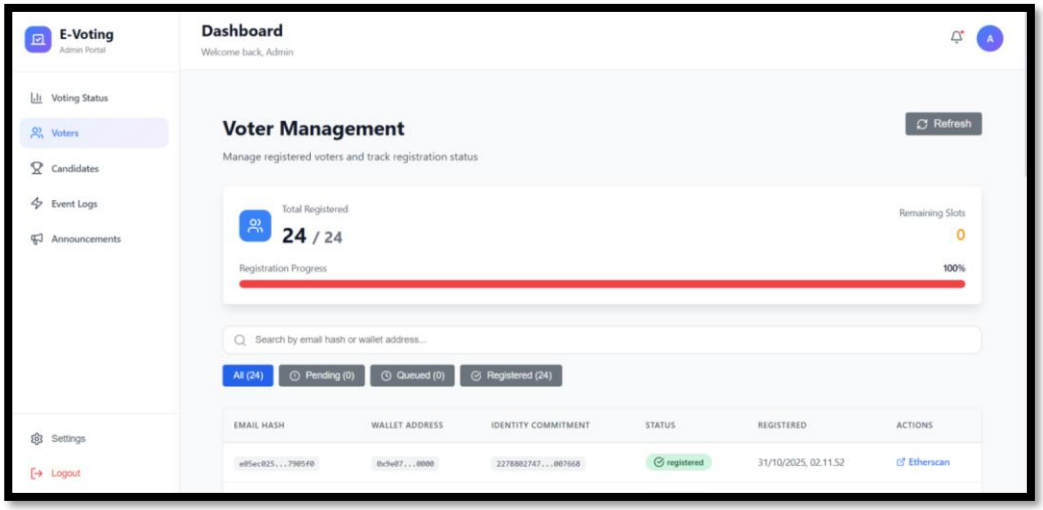
menampilkan dashboard admin dengan status siklus voting, yaitu Started, Paused, dan Stopped. Melalui halaman ini, admin dapat memantau jumlah suara dan mengatur jalannya proses e-voting secara real-time



Gambar 4 *Page voting* status *lifecycle. Started, and Stopped*

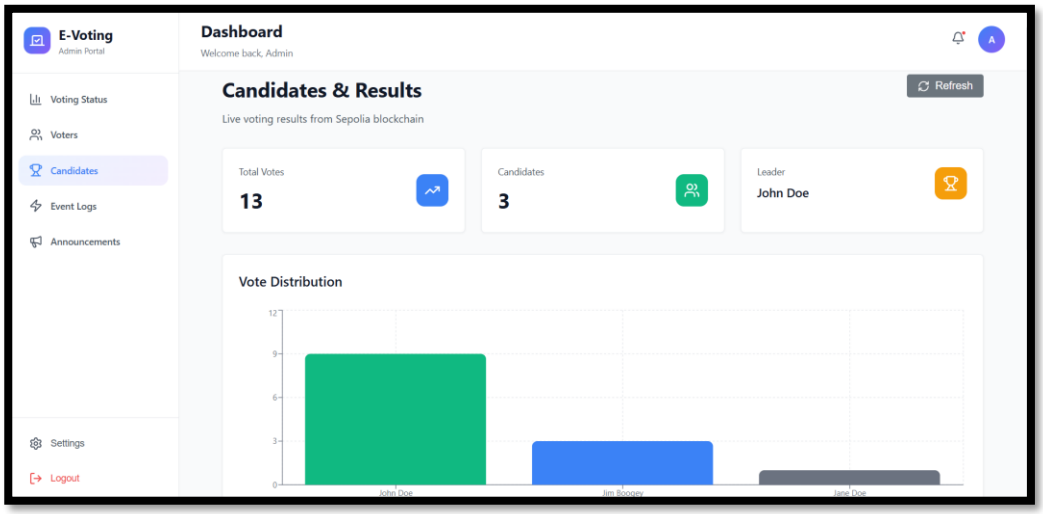
Gambar 5 ini menunjukkan halaman manajemen pemilih (Voter Management) pada dashboard admin. Halaman ini digunakan untuk memantau jumlah pemilih yang telah terdaftar dan status registrasinya. Admin dapat melihat berapa banyak pemilih aktif, belum terdaftar, atau yang telah menyelesaikan proses registrasi. Fitur ini membantu memastikan bahwa seluruh pemilih yang berhak sudah terdaftar dengan benar sebelum proses voting dimulai.

Jurnal Minfo Polgan
Volume 14, Nomor 2, November 2025
DOI : https://doi.org/10.33395/jmp.v14i2.15536
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 5 *Page* untuk memonitor *voters*

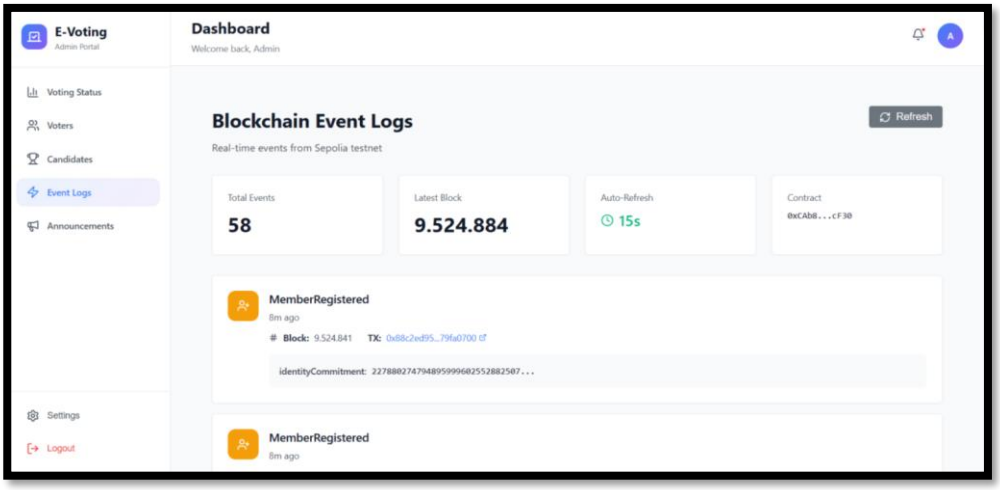
Pada Gambar 6 menunjukkan halaman dashboard admin yang digunakan untuk memantau hasil perolehan suara dari tiga kandidat. Tampilan memperlihatkan jumlah suara yang diterima masing-masing kandidat serta distribusi suara dalam bentuk grafik batang (vote distribution). Fitur ini berfungsi agar admin dapat melihat hasil voting secara real-time yang diperoleh langsung dari blockchain tanpa harus mengakses database manual. Dengan demikian, transparansi dan akurasi hasil pemilihan dapat terjamin.



Gambar 6 *Page* untuk memonitor ke-3 kandidat

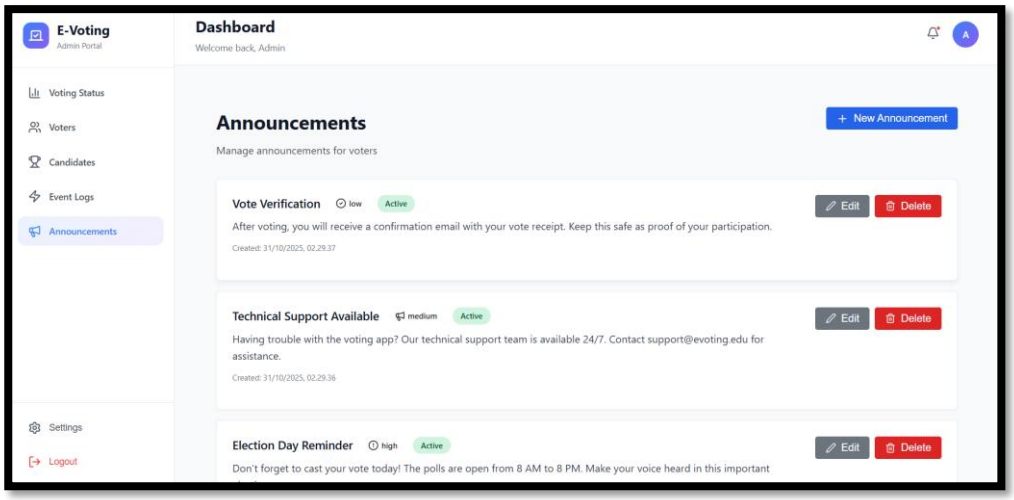
Gambar 7 ini menunjukkan halaman Blockchain Event Logs pada dashboard admin. Halaman ini digunakan untuk memantau aktivitas transaksi (tx) yang terjadi di smart contract, seperti pendaftaran anggota atau pencatatan suara.

Jurnal Minfo Polgan
Volume 14, Nomor 2, November 2025
DOI : https://doi.org/10.33395/jmp.v14i2.15536
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 7 *Page* untuk memonitor tx di *smart contract*

Informasi yang tampil meliputi jumlah blok, nomor blok terakhir, waktu eksekusi transaksi, dan event yang tercatat. Fitur ini memastikan bahwa setiap proses voting benar-benar tersimpan di blockchain dan dapat diaudit secara transparan.



Gambar 8 *Page* untuk *push* pengumuman ke aplikasi *user*

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dan pengujian system yang dikembangkan, Adapun Kesimpulan pada penelitian ini sebagai berikut:

1. Sistem yang dikembangkan berhasil memanfaatkan teknologi blockchain untuk mencatat setiap suara secara permanen, transparan, dan tidak dapat diubah. Setiap transaksi voting tercatat pada jaringan blockchain sehingga mencegah kecurangan dan manipulasi data. Dengan demikian, rancangan sistem ini terbukti mampu menjamin keamanan dan integritas suara dalam proses pemilihan elektronik.
2. Implementasi autentikasi biometrik sidik jari memberikan lapisan keamanan tambahan yang memastikan bahwa hanya pemilih sah yang dapat memberikan suara. Proses verifikasi dilakukan melalui fitur BiometricPrompt API pada Android, sehingga identitas pemilih dapat diverifikasi secara unik dan tidak dapat dipalsukan.

3. Berdasarkan hasil pengujian, aplikasi e-voting menunjukkan kinerja yang baik dengan proses login, verifikasi, dan voting berjalan lancar tanpa error. Sistem dinilai aman, efisien, dan mudah digunakan, baik dari sisi antarmuka maupun fungsionalitas. Pengguna dapat dengan mudah melakukan pendaftaran, verifikasi OTP, dan pemungutan suara secara cepat dan aman.

UCAPAN TERIMA KASIH

Terima kasih kepada tempat mengabdi kami di Politeknik Negeri Sriwijaya yang sudah memberikan motivasi terhadap kami dan terima kasih kepada keluarga kami yang paling kami sayangi.

REFERENSI

Asrul, A., Putra, A. ., & Rajab, M. . (2025). Transpormasi Bisnis Di Era Digital: Peluang, Tantangan, Dan Strategi Inovasi. *Jurnal Minfo Polgan*, *13*(2), 2294-2298.

Asrul, A. (2024). Penerapan Strategi Manajemen Teknologi untuk Meningkatkan Daya Saing di Industri 4.0. *INVESTASI : Inovasi Jurnal Ekonomi Dan Akuntansi*, *2*(4), 215–220.

Asrul, A., Windayani, W., Putra, A. ., Bahar, H. ., Baihaqi, B., Ladianto, A. J. ., Pebrianti, H. ., & Qadri, M. S. . (2025). Pemanfaatan Big Data Analytics dalam Proses Manajemen Teknologi untuk Prediksi Permintaan Pasar. *Jurnal Minfo Polgan*, *13*(2), 2433-2438.

W. Xue, Y. Yang, Y. Li, H. H. Pang, and R. H. Deng, "ACB-Vote: Efficient, Flexible, and Privacy-Preserving Blockchain-Based Score Voting with Anonymously Convertible Ballots," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 3720–3734, 2023.

G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application within IoT-Oriented Smart Cities," IEEE Access, vol. 9, pp. 34165–34176, 2021.

C. McCabe, A. I. C. Mohideen, and R. Singh, "A Blockchain-Based Authentication Mechanism for Enhanced Security," Sensors, vol. 24, no. 17, Art. 5830, 2024.

A. Jamal, Q. Abbas, and S. Ali, "Blockchain-Based Identity Verification System Using a Permissioned Ledger," in Proc. 2024 Int. Conf. on Emerging Technologies, 2024, pp. 1–6.

S. Swar, S. Shinde, P. Nimkar, A. B. S. K. Reddy, and T. Lotlikar, "Cryptcast: E-Voting System Utilizing Blockchain," in Proc. 6th Int. Conf. on Advances in Science and Technology (ICAST), 2023, pp. 1–5.

A. Al-Ismaili, Y. Al-Mulla, and M. Al-Salih, "A Blockchain-Based E-Voting System Model for Oman Utilizing Biometric Verification," in Proc. Int. Conf. on Innovative Blockchain Technology, 2024, pp. 120–127.

M. R. Ahmed, A. Dhar, R. A. Shaikh, A. Shahid, and M. A. Imran, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," IEEE Access, vol. 10, pp. 113434–113459, 2022.

T. Subburaj, K. S. Raju, K. Suthendran, K. P. Kumar, C. Rekha, S. Sultana, and C. Deeraj, "Biometric Authentication with Blockchain: A Secure and User-Friendly Approach," in Intelligent Systems and Sustainable Computing, Springer, 2025, pp. 513–522.

S. AbdulKather, P. Patel, and P. J. Rodrigues, "A Lightweight Blockchain Framework for Secure and Transparent E-Voting," in Proc. 2024 Int. Conf. on Blockchain and Cryptography (ICBCrypto), 2024, pp. 45–52.

N. Saxena, "Blockchain as a Governance Layer for AGI Ethics," Scientific Journal of Artificial Intelligence and Blockchain Technologies, vol. 2, no. 1, pp. 88–96, 2025.

e-ISSN : 2797-3298
p-ISSN : 2089-9424

Z. Liu, X. Zhang, L. Lao, G. Li, and B. Xiao, "DBE-voting: A Privacy-Preserving and Auditable Blockchain-Based E-Voting System," in Proc. IEEE Int. Conf. on Communications (ICC), Rome, Italy, 2023, pp. 6571–6577.

S. Panja and B. K. Roy, "A Secure End-to-End Verifiable E-Voting System Using Blockchain and Cloud Server," Journal of Information Security and Applications, vol. 59, Art. 102815, Jun. 2021.

K. Hegadekatti, "Design of a Secure Electronic Voting System Based on Zero-Knowledge Proof and Blockchain Technology," Int. J. of Electronic Governance, vol. 14, no. 1, pp. 1–20, 2022.

H. Q. Flayyih, J. Waleed, and A. M. Ibrahim, "A Privacy-Preserving E-Voting System Using Federated Learning and CNNs for Secure Fingerprint and Biometric Verification," Diyala Journal of Engineering Sciences, vol. 18, no. 1, Mar. 2025.

A. M. Al-Hashedi, A. A. Al-Qaness, and M. A. Al-Qaness, "Enhancing E-Voting Security with Blockchain and Decentralized Random Number Generation," BPAS Journals, vol. 12, no. 2, pp. 10–22, 2024.

M. A. Bazzi, A. Spanos, and I. Kantzavelou, "Z-Voting: A Zero Knowledge Based Confidential Voting on Blockchain," in Proc. 2023 Int. Conf. on Software Engineering and Machine Learning, 2023, pp. 328–334.

M. Alzamel, L. S. Choo, and A. B. M. Zeki, "A Secure End-to-End Verifiable E-Voting System Using Zero-Knowledge Proof and Blockchain," IEEE Access, vol. 9, pp. 102345–102358, 2021.

A. G. P. D. Ge, "Optimizing Smart Contract Development: A Practical Model for Gasless Transactions via Facial Recognition in Blockchain," Int. J. of Multidisciplinary Research and Growth Evaluation, vol. 3, no. 1, pp. 978–989, Jan. 2022.

A. Werth, M. Pahl, and N. El Ioini, "A Comprehensive Review of Zero-Knowledge Proofs in Distributed Systems," Security and Communication Networks, vol. 2023, Article ID 9843217, 18 pages, 2023.

S. S. Sameera et al., "Privacy-Preserving in Blockchain-Based Federated Learning Systems," Computer Communications, vol. 222, pp. 38–67, 2024.

O. A. Ogunnowo, A. A. A. G. Elnashar, and K. Kapoor, "Blockchain-Based E-Voting Systems: A Technology Review," Electronics, vol. 13, no. 1, p. 17, Jan. 2024.

K. A. Al-Saqqar, "Electronic Voting System: Nature, Origin and Its Global Application," Int. J. of Innovation, Creativity and Change, vol. 15, no. 2, pp. 200–215, 2021.

M. Werth, J. Pahl, and N. El Ioini, "Biometric Authentication in Android: Enhancing Security with AI-Powered Solutions," Asian Journal of Research in Computer Science, vol. 18, no. 4, pp. 1–15, 2025.

I. Dogan, M. Schaub, and L. Badr, "Blockchain-Based Anonymous Reputation System for Performance Appraisal," IEEE Access, vol. 11, pp. 1–14, 2023.

A. K. M. M. R. Islam, "A Comparative Study on Blockchain Based E-Voting Systems," International Journal of Computer Applications, vol. 184, no. 12, pp. 1–8, 2022.

Privacy and Scaling Explorations (PSE), "Semaphore V4 Specification," GitHub Repository, 2024. [Online]. Available: https://github.com/ZKspecs/ZKspecs/blob/main/specs/3/README.md (diakses 26 Okt 2025).

Android Developers, "Android Keystore System," Android Developer Reference, 2025. [Online]. Available: https://developer.android.com/privacy-and-security/keystore (diakses 26 Okt 2025).

e-ISSN : 2797-3298
p-ISSN : 2089-9424

Polygon Technology, "Meta Transactions," Polygon Docs, 2024. [Online]. Available: https://docs.polygon.technology/pos/concepts/transactions/meta-transactions/ (diakses 26 Okt 2025).

A. Spanos and I. Kantzavelou, "EtherVote: A Secure Smart Contract-Based E-Voting System," in Proc. 2022 IEEE Int. Conf. on Blockchain and Cryptocurrency (ICBC), 2022, pp. 1–5.