Jurnal Penelitian Inovatif (JUPIN)
Vol. 6, No. 5, November 2026, Hal. 4093-4104
https://jurnal-id.com/index.php/jupin

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Implementasi Sistem *E-Voting* Pemilihan Presiden Mahasiswa Universitas Halu Oleo Berbasis *Blockchain* dengan Metode Kriptografi SHA-256

Diki Ardika Wiratama*[1], La Ode Muhammad Golok Jaya[2], Bambang Pramono[3]

[1,2,3] Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Indonesia
Email: [1]ardykaaw26@gmail.com, [2]laodemgj@uho.ac.id, [3]bambang.pramono@uho.ac.id

Abstrak

Pelaksanaan Pemilihan Presiden Mahasiswa dalam Pemilihan Umum Raya Mahasiswa (PEMIRA) di Universitas Halu Oleo (UHO) menghadapi krisis kepercayaan akibat kelemahan arsitektur sistem *e-voting* terpusat yang rentan terhadap *Single Point of Failure* (SPoF), *Single Point of Trust* (SPoT), dan manipulasi *internal* basis data. Penelitian ini bertujuan mengimplementasikan sistem pemungutan suara elektronik (e-voting) terdesentralisasi dengan metode kriptografi SHA-256 berbasis *blockchain Ethereum Sepolia* dan *smart contract* untuk verifikasi suara pemilih. Sistem dikembangkan menggunakan model *Waterfall* dengan arsitektur hibrida tiga lapisan: lapisan off-chain untuk manajemen DPT dan autentikasi pemilih, lapisan gasless *relayer* untuk meniadakan beban *gas fee* dan kerumitan dompet *Web3* bagi mahasiswa, serta lapisan on-chain (*smart contract Solidity* PemiraUHO.sol) untuk pencatatan intisari hak suara secara kekal (*immutable ledger*). Untuk menjamin kerahasiaan pilihan, setiap suara dienkapsulasi menggunakan *hashing* SHA-256 dengan penambahan *cryptographic salt* 32-byte guna menerbitkan tanda terima digital (*digital vote receipt*) untuk verifikasi mandiri (*individual verifiability*). Pengujian fungsional *Black Box* membuktikan 10 dari 10 skenario berhasil (100%). Pengujian kinerja kriptografi SHA-256 menghasilkan rata-rata perubahan bit keluaran sebesar 52,19% dari lima skenario mutasi bit masukan yang berfluktuasi di sekitar nilai acuan teoritis 50%. Pengujian audit integritas data membuktikan sistem mampu mendeteksi empat dari empat perubahan data simulasi secara deterministik melalui pencocokan catatan lokal dengan catatan *Sepolia*. Evaluasi *User Acceptance Testing* (UAT) menghasilkan persentase kelayakan 88,40% dari 10 responden pemangku kepentingan. Kontribusi penelitian ini memperlihatkan keandalan integrasi *blockchain* dan tanda terima digital dalam menyediakan bukti pencatatan transaksi yang transparan dan dapat diverifikasi secara mandiri.

Kata kunci: *avalanche effect*, *blockchain*, *e-voting*, *ethereum sepolia*, sha-256, *smart contract*

Abstract

The implementation of the Student Executive Board Presidential Election (PEMIRA) at Universitas Halu Oleo (UHO) faces a crisis of trust caused by architectural vulnerabilities in centralized e-voting systems, specifically Single Point of Failure (SPoF), Single Point of Trust (SPoT), and internal database tampering. This study aims to implement a decentralized electronic voting (e-voting) system using SHA-256 cryptographic method based on Ethereum Sepolia blockchain and smart contracts for voter ballot verification. The system was developed using the Waterfall lifecycle within a three-tier hybrid architecture: an off-chain layer for voter registry and authentication, a gasless relayer layer eliminating gas fee burdens and Web3 wallet complexities for student voters, and an on-chain ledger layer (Solidity smart contract PemiraUHO.sol) for immutable vote logging. To enforce ballot privacy, each vote payload is encapsulated via SHA-256 hashing with a 32-byte cryptographic salt to issue a digital vote receipt for individual verifiability. Black Box functional testing achieved success in 10 out of 10 scenarios (100%). Cryptographic evaluation of SHA-256 demonstrated an average output bit variation of 52.19% across five input bit mutation scenarios, fluctuating around the theoretical 50% benchmark. Data integrity audit simulations proved the system deterministically detected four out of four simulated data tampering cases by matching local database records with Sepolia logs. User Acceptance Testing (UAT) yielded a feasibility score of 88.40% from 10 representative stakeholders. The primary contribution of this research demonstrates the reliability of blockchain integration and digital vote receipts in providing transparent, independently verifiable transaction recording for student elections.

Keywords: *avalanche effect, blockchain, e-voting, ethereum sepolia, sha-256, smart contract*

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

1. PENDAHULUAN

Demokrasi di lingkungan perguruan tinggi merupakan representasi miniatur tata kelola kenegaraan yang mengedepankan kedaulatan mahasiswa dalam menentukan arah kepemimpinan organisasi kemahasiswaan. Di Universitas Halu Oleo (UHO), perwujudan kedaulatan tersebut diselenggarakan melalui Pemilihan Umum Raya Mahasiswa (PEMIRA) guna memilih Presiden Mahasiswa dan representasi kelembagaan kemahasiswaan. Pelaksanaan suksesi kepemimpinan ini diatur secara formal melalui Peraturan Rektor Universitas Halu Oleo Nomor 1 Tahun 2023 tentang Pedoman Tata Kelola Organisasi Kemahasiswaan dan Tata Cara Pemilihan Raya Mahasiswa (Universitas Halu Oleo, 2023). Seiring dengan masifnya populasi civitas akademika UHO yang mencapai lebih dari 35.000 mahasiswa aktif dari berbagai jenjang pendidikan, panitia pemilihan telah bertransformasi meninggalkan bilik suara manual berbasis kertas menuju adopsi sistem pemungutan suara elektronik (*e-voting*) berbasis web guna memangkas biaya logistik serta mempercepat waktu rekapitulasi penghitungan suara.

Meskipun menawarkan efisiensi operasional yang nyata, implementasi sistem *e-voting* yang berjalan saat ini masih mengadopsi paradigma arsitektur *client-server* konvensional dengan pengelolaan basis data terpusat (centralized database). Karakteristik tertutup pada basis data terpusat menimbulkan kerentanan struktural yang sangat fatal, yaitu *Single Point of Failure* (SPoF) dan *Single Point of Trust* (SPoT). Kerentanan ini membuka celah ancaman *internal* (*insider threats*) yang tidak dapat dimitigasi oleh mekanisme kontrol akses biasa, di mana administrator basis data yang memiliki hak akses istimewa (privileged user) dapat melakukan modifikasi, penghapusan, atau penyisipan baris data pemungutan suara secara sepihak tanpa meninggalkan jejak audit yang dapat diverifikasi secara independen oleh publik. Ketiadaan transparansi ini kerap menimbulkan ketidakpercayaan pemilih terhadap integritas perolehan suara yang berujung pada eskalasi sengketa persidangan di Mahkamah Sengketa Organisasi Kemahasiswaan (MSOK) UHO, aksi boikot dari berbagai fakultas, serta tingginya angka golongan putih (golput) akibat skeptisisme mahasiswa terhadap kejujuran sistem pemilihan (Universitas Halu Oleo, 2023).

Urgensi penyelesaian krisis transparansi ini diperkuat secara empiris oleh temuan penelitian Mubbaraq, Ransi, dan Hamundu (2024) mengenai analisis penggunaan aplikasi *e-voting* PEMIRA UHO dengan kerangka *Technology Acceptance Model* (TAM). Dalam penelitian tersebut dibuktikan secara statistik bahwa variabel Kepercayaan terhadap Internet dan Sistem (*Trust in Internet*) memegang peranan sangat krusial sebagai variabel moderator, dengan kontribusi pengaruh mencapai 97,3% terhadap niat perilaku mahasiswa (Behavioral Intention to Use) untuk berpartisipasi dalam sistem *e-voting*. Temuan statistik tersebut juga mengungkapkan bahwa hipotesis pengaruh langsung persepsi kemudahan penggunaan (Perceived Ease of Use) terhadap niat memilih ditolak apabila tidak disertai oleh rasa percaya (trust) terhadap integritas sistem (Mubbaraq dkk., 2024). Fakta empiris ini menegaskan bahwa secanggih atau semudah apa pun antarmuka sistem *e-voting* yang dibangun, partisipasi aktif mahasiswa tidak akan pernah tercapai secara optimal selama sistem pemilihan beroperasi di atas infrastruktur tertutup yang rawan manipulasi *internal*.

Dalam diskursus teknologi informasi nasional dan internasional, pemanfaatan teknologi *blockchain* muncul sebagai paradigma komputasi mutakhir untuk mengatasi kegagalan integritas sistem terpusat (Ananda dkk., 2024). *Blockchain* beroperasi di atas prinsip buku besar terdistribusi (*distributed ledger*) yang diamankan oleh konsensus kriptografis dan jaringan simpul *peer-to-peer* (Nakamoto, 2008; Buterin, 2014; Antonopoulos & Wood, 2018). Setiap blok transaksi saling terikat secara kronologis melalui nilai *hash* kriptografis yang membentuk rantai data yang kekal (*immutable*) dan tahan terhadap manipulasi (*tamper-proof*) (Bashir, 2020; Tas & Tanriöver, 2020). Selain itu, kehadiran kontrak pintar (*smart contract*) memungkinkan logika verifikasi dan penghitungan suara dieksekusi secara otonom dan deterministik tanpa ketergantungan pada pihak ketiga (Al-Saegh & Al-Hakeem, 2023; Sadia dkk., 2019; Latif dkk., 2022; Aripin & Muttaqin, 2025; Arianto dkk., 2021).

Namun demikian, penerapan *blockchain* pada sistem pemilu elektronik memerlukan mitigasi mendalam terhadap aspek kerahasiaan pilihan pemilih (*ballot secrecy*). Sebagaimana diingatkan dalam kajian kritis Park, Specter, Narula, dan Rivest (2021), sifat keterbukaan publik (transparency) pada buku besar *blockchain* berisiko mengekspos pilihan politik pemilih apabila data suara dicatat secara transparan tanpa enkapsulasi kriptografis yang memadai. Sejumlah penelitian terdahulu telah berupaya

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

menjawab tantangan ini pada ranah pemilu mahasiswa. Kelarno dan Widayat (2024) mengimplementasikan kontrak pintar pada sistem *e-voting* pemilihan mahasiswa di Universitas Gadjah Mada; akan tetapi, penelitian tersebut masih membebankan interaksi *Web3* yang rumit kepada mahasiswa awam (kebutuhan dompet digital dan biaya *gas*) serta belum menyediakan tanda terima audit yang diperkuat garam kriptografis. Di sisi lain, Kalyani, Modadugu, dan Neelima (2025) merancang pemungutan suara terdesentralisasi menggunakan algoritma *Secure Hash Algorithm 256-bit* (SHA-256) dengan pengenalan wajah, namun sistem tersebut belum memiliki modul rekonsiliasi audit data otomatis untuk membuktikan inkonsistensi data lokal terhadap *ledger blockchain* serta belum mengintegrasikan pola transaksi tanpa biaya (gasless) bagi pemilih (Kalyani dkk., 2025; Tedyyana dkk., 2024).

Guna menutup kesenjangan teknis tersebut, penelitian ini mengusulkan kebaruan (novelty) melalui perancangan arsitektur hibrida tiga lapisan yang memadukan keunggulan manajemen data terpusat (off-chain), kemudahan akses bebas biaya melalui Gasless *Relayer* Pattern berbasis *Ethers.js* v6, serta kekekalan pencatatan terdesentralisasi pada jaringan *Ethereum Sepolia Testnet*. Pengamanan hak suara diperkuat dengan enkapsulasi kriptografi SHA-256 bergaram kriptografis (*cryptographic salt*) 32-byte untuk menerbitkan tanda terima digital (*digital vote receipt*) yang memfasilitasi verifikasi mandiri pemilih (*individual verifiability*). Penelitian ini bertujuan untuk mengembangkan sistem pemungutan suara elektronik terdesentralisasi yang menjamin verifikasi suara dan integritas data pada Pemilihan Presiden Mahasiswa UHO, dengan aspek yang diuji meliputi pengujian fungsionalitas *Black Box*, kinerja matematis efek longsoran (*avalanche effect*) algoritma SHA-256, pengujian integritas audit data on-chain vs off-chain, serta evaluasi penerimaan pengguna akhir melalui *User Acceptance Testing* (UAT).

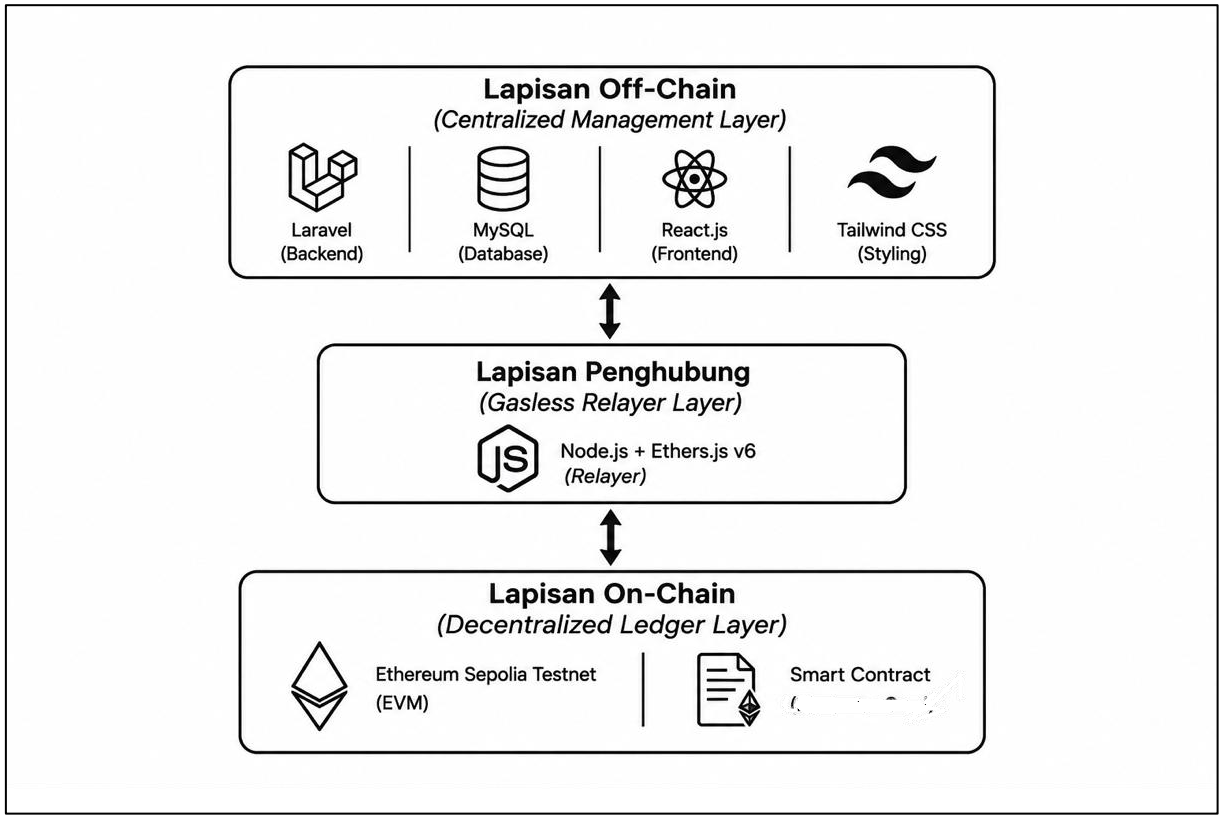
2. METODE PENELITIAN

Metode rekayasa perangkat lunak yang diterapkan dalam penelitian ini mengadopsi model *Waterfall* klasik yang mencakup tahapan terstruktur secara linier: Analisis Kebutuhan (Requirements Analysis), Perancangan Sistem (System Design), Implementasi Sistem (Coding), dan Pengujian Sistem (Testing) (Pressman & Maxim, 2020; Sommerville, 2016). Pemilihan model *Waterfall* sangat krusial mengingat karakteristik fundamental dari *smart contract* pada *blockchain* bersifat kekal (*immutable*), di mana kode program yang telah digelar (deployed) ke jaringan publik tidak dapat disunting kembali tanpa migrasi kontrak yang berisiko tinggi. Oleh karena itu, tahapan analisis dan perancangan harus diselesaikan secara tuntas sebelum implementasi. Dalam lingkup penelitian skripsi ini, tahapan diselesaikan hingga pengujian dan evaluasi empiris sistem, sedangkan tahap pemeliharaan sistem (maintenance) merupakan fase operasional jangka panjang yang berada di luar cakupan penelitian ini.

Analisis kebutuhan sistem dirumuskan berdasarkan tiga sumber data primer dan sekunder: (1) observasi lapangan terhadap dinamika penyelenggaraan PEMIRA UHO di lingkungan kampus, (2) studi dokumentasi regulasi kemahasiswaan pada Peraturan Rektor Universitas Halu Oleo Nomor 1 Tahun 2023, serta (3) data simulasi Daftar Pemilih Tetap (DPT) yang bersumber dari struktur portal Sistem Informasi Akademik (SIAKAD) UHO yang mencakup representasi mahasiswa aktif dari tujuh fakultas (Fakultas Teknik, FKIP, FEB, FISIP, Fakultas Hukum, Fakultas Pertanian, dan FMIPA). Kebutuhan fungsional utama mencakup autentikasi pemilih berbasis NIM, validasi pencegahan pencoblosan ganda (*double-voting*), enkapsulasi pilihan suara dengan SHA-256 dan *salt* 32-byte, transaksi bebas biaya *gas* melalui *relayer*, serta modul verifikasi audit suara on-chain.

Sistem *e-voting* yang dikembangkan menerapkan arsitektur hibrida (hybrid architecture) yang memisahkan beban komputasi dan penyimpanan data ke dalam tiga lapisan terkoordinasi: lapisan off-chain, lapisan gasless *relayer*, dan lapisan on-chain, sebagaimana diilustrasikan pada Gambar 1. Perlu ditekankan secara konsisten bahwa dalam model hibrida ini, buku besar *Ethereum Sepolia* berfungsi secara eksklusif untuk pencatatan transaksi kekal dan log audit hak suara, sedangkan pengelolaan daftar pemilih, proses autentikasi login, serta pengiriman paket transaksi ke jaringan uji *Sepolia* masih bergantung pada komponen peladen yang dikelola oleh panitia penyelenggara.

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366



Gambar 1. Arsitektur Hibrida Sistem *E-Voting* Berbasis *Blockchain Ethereum* dan SHA-256

Rincian tanggung jawab fungsional dari ketiga lapisan arsitektur hibrida tersebut adalah sebagai berikut: (1) Lapisan Off-Chain (*Web2*) dibangun menggunakan *framework Laravel* 10, *MySQL* 8.0, *Inertia.js*, *React.js*, dan *Tailwind CSS*. Lapisan ini bertanggung jawab melayani antarmuka bilik suara digital yang responsif, manajemen data DPT, autentikasi kredensial mahasiswa berbasis NIM dan kata sandi terenkripsi, serta pembentukan berkas *payload JSON* suara pemilih. (2) Lapisan Gasless *Relayer* (*Middleware*) dioperasikan menggunakan *runtime Node.js* dan pustaka *Ethers.js* v6. Modul ini berperan sebagai penandatangan transaksi (transaction *signer*) perantara yang menanggung seluruh biaya *gas fee* transaksi pemungutan suara menggunakan dompet sistem resmi KPU-M, sehingga mahasiswa dapat mencoblos tanpa memerlukan kepemilikan dompet kripto (*Web3 wallet*) maupun saldo mata uang kripto. (3) Lapisan On-Chain (*Web3*) bertumpu pada kontrak pintar *Solidity* 0.8.20 (PemiraUHO.sol) yang digelar pada jaringan uji publik *Ethereum Sepolia Testnet*. Kontrak pintar ini mencatat intisari hak suara secara terdesentralisasi, mengeksekusi logika pencegahan pemilih ganda secara otonom, dan mengunci rekapitulasi perolehan suara tanpa kendali administratif sepihak.

Untuk menjamin kerahasiaan pilihan (*ballot secrecy*) sekaligus menyediakan auditabilitas mandiri (*individual verifiability*), pilihan suara dienkapsulasi menggunakan fungsi *hash* kriptografi *Secure Hash Algorithm 256-bit* (SHA-256) sesuai standar FIPS 180-4 (National Institute of Standards and Technology, 2015). SHA-256 bekerja dengan memproses pesan masukan M dalam blok-blok 512-bit setelah melalui tahapan penambahan bit pengganjal (*padding*) dengan aturan:

$$L + 1 + k \equiv 448 \, (mod \, 512) \quad (1)$$

Di mana L merepresentasikan panjang pesan masukan dalam satuan bit, angka 1 merupakan penambahan satu bit '1' di akhir pesan, dan k adalah jumlah bit '0' terkecil tak-negatif yang diperlukan agar panjang total kongruen dengan 448 *modulo* 512. Selanjutnya, panjang pesan asli L dikodekan ke dalam format biner 64-bit dan dilekatkan di akhir blok sehingga menghasilkan panjang pesan yang merupakan kelipatan tepat 512 bit. Selama 64 putaran kompresi *internal*, fungsi logika *Choice* (Ch) dan *Majority* (Maj) dieksekusi secara deterministik menggunakan operasi bitwise:

$$Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z) \quad (2)$$

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \quad (3)$$

Setiap putaran menghasilkan pembaruan terhadap delapan variabel kerja 32-bit (a hingga h) berdasarkan dua konstanta pengendali:

$$T_1 = h + \sum_1(e) + ch(e, f, g) + K_t + W_t, \; T_2 = \sum_0(a) + Maj(a, b, c) \quad (4)$$

Guna menangkal serangan tabel pelangi (*rainbow table* attack) dan serangan kamus (dictionary attack) akibat rendahnya variasi pilihan paslon (hanya paslon 1 atau 2), sistem mengintegrasikan penambahan *cryptographic salt* acak sebesar 32-byte (256-bit). Struktur *payload* suara memadukan candidate_id, random_salt, timestamp, dan UUID transaksi. Melalui skema ini, diterbitkan dua *token* kriptografis: *token* audit (T_audit) yang disimpan secara off-chain dan *token* transaksi (T_token) yang diserahkan kepada pemilih sebagai tanda terima digital (*digital vote receipt*) untuk memantau status rekaman suara pada penjelajah blok *Etherscan Sepolia*.

Prosedur pengujian sistem dirancang secara komprehensif mencakup empat metodologi evaluasi: (1) Pengujian Fungsionalitas *Black Box*: Dilakukan terhadap 10 skenario fungsionalitas mencakup autentikasi, pembatasan hak pilih, pencatatan transaksi *relayer*, dan validasi *smart contract* dengan kriteria keberhasilan kesesuaian mutlak antara masukan dan luaran berdasarkan teknik *Boundary Value Analysis* (Mustaqbal dkk., 2015). (2) Pengujian Kinerja Kriptografi Efek Longsoran (*Avalanche Effect*): Menguji sensitivitas difusi algoritma SHA-256 terhadap lima pasangan masukan data pemira dengan rancangan mutasi terkontrol tepat satu bit atau satu karakter (modifikasi candidate_id, pergeseran stempel waktu 1 detik, mutasi satu karakter *salt*, penyisipan spasi, dan modifikasi UUID transaksi). Persentase efek longsoran dihitung dengan mengukur jumlah bit biner keluaran yang berbalik (*bit flipping*) dari total 256 bit:

$$AE = \frac{D}{N} \times 100\% \quad (5)$$

Di mana AE adalah persentase *Avalanche Effect*, D adalah jumlah bit keluaran yang berubah, dan N adalah panjang total bit *hash* keluaran (256 bit). Nilai 50% dijadikan sebagai nilai acuan teoretis ideal yang mengindikasikan sifat keacakan sempurna. (3) Pengujian Integritas Data On-Chain vs Off-Chain: Mensimulasikan empat skenario manipulasi paksa pada tabel basis data lokal off-chain (pemalsuan nomor paslon, pengubahan *hash* suara lokal, manipulasi *token* audit, dan injeksi baris suara palsu) serta satu skenario normal valid. Pengujian ini mengukur kemampuan sistem audit dalam mendeteksi anomali data secara deterministik. (4) Pengukuran Waktu Transaksi: Diukur dari titik awal saat modul *relayer* mengeksekusi *sendTransaction*() ke *mempool* jaringan *Sepolia* hingga diterbitkannya bukti tanda terima blok transaksi (transaction receipt block *mined*) pada 10 transaksi pengujian berturut-turut.

(5) Evaluasi Penerimaan Pengguna (*User Acceptance Testing* / UAT): Instrumen kuesioner UAT disusun mengacu pada perluasan kerangka kerja *Technology Acceptance Model* (TAM) dan standar ISO/IEC 25010, mencakup 10 butir instrumen pernyataan terstruktur (P1–P10) yang disajikan pada Tabel 1. Penilaian mengadopsi Skala Likert 5 poin terbobot: Sangat Setuju (SS = 5), Setuju (S = 4), Cukup Setuju/Netral (CS = 3), Tidak Setuju (TS = 2), dan Sangat Tidak Setuju (STS = 1) (Sugiyono, 2019). Pemilihan responden melibatkan 10 orang pemangku kepentingan representatif PEMIRA UHO yang terdiri dari: satu Administrator KPU-M (selaku operator teknis sistem), dua Saksi Pasangan Calon (selaku pengawas integritas suara paslon 1 dan paslon 2), serta tujuh Mahasiswa Pemilih yang mewakili sebaran tujuh fakultas di lingkungan Universitas Halu Oleo (Fakultas Teknik, FKIP, FEB, FISIP, Fakultas Hukum, Fakultas Pertanian, dan FMIPA). Persentase skor kelayakan penerimaan dihitung menggunakan formulasi standar:

$$Persentase\ Kelayakan = \left(\frac{\sum Skor\ Aktual}{\sum Skor\ Maksimal}\right) \quad (6)$$

Hasil persentase kelayakan UAT diinterpretasikan ke dalam skala kelayakan standar menurut Sugiyono (2019): rentang 81%–100% (Sangat Layak), 61%–80% (Layak), 41%–60% (Cukup Layak), 21%–40% (Kurang Layak), dan 0%–20% (Sangat Tidak Layak). Rincian matriks instrumen butir kuesioner UAT disajikan pada Tabel 1.

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Tabel 1. Matriks Instrumen Pernyataan Kuesioner *User Acceptance Testing* (UAT)

No.	Kode	Pernyataan Evaluasi Pengguna (Instrumen UAT)	Dimensi Pengukuran
1	P1	Antarmuka sistem *e-voting* PEMIRA UHO memiliki tata letak yang bersih, rapi, dan mudah dipahami.	Kemudahan (Ease of Use)
2	P2	Proses autentikasi login menggunakan NIM dan kata sandi berjalan cepat dan tanpa kendala teknis.	Kemudahan (Ease of Use)
3	P3	Informasi nomor urut, foto resmi berjas almamater, dan visi-misi pasangan calon tersaji secara jelas.	Kemanfaatan (Usefulness)
4	P4	Proses mencoblos di bilik suara digital sangat praktis dan dialog konfirmasi mencegah salah klik.	Kemudahan (Ease of Use)
5	P5	Penerbitan tanda terima digital (receipt) memberikan kepastian dan rasa aman bahwa hak suara dicatat.	Kepercayaan (Trust)
6	P6	Tautan verifikasi ke *Etherscan Sepolia* memudahkan mahasiswa memantau status pencatatan transaksi secara mandiri.	Transparansi (Transparency)
7	P7	Sistem *e-voting* terdesentralisasi ini jauh lebih efektif dan hemat waktu dibandingkan pemilihan kertas konvensional.	Kemanfaatan (Usefulness)
8	P8	Penerapan enkripsi SHA-256 dan *blockchain* membuat saya percaya bahwa suara saya tidak dapat dimanipulasi pihak lain.	Keamanan (Security)
9	P9	Mekanisme gasless voting membuat proses pemilihan sangat nyaman tanpa perlu repot memiliki saldo aset kripto.	Kemudahan (Ease of Use)
10	P10	Secara keseluruhan, saya setuju sistem *e-voting blockchain* ini diadopsi pada PEMIRA UHO yang sebenarnya.	Penerimaan Akhir (Acceptance)

3. HASIL DAN PEMBAHASAN

3.1. Implementasi Lingkungan Perangkat Lunak dan *Smart Contract*

Sistem *e-voting* berhasil diimplementasikan pada lingkungan peladen terintegrasi dengan *runtime* PHP 8.2 (*Laravel* 10), *Node.js* v20, basis data *MySQL* 8.0, *framework Tailwind CSS*, dan pustaka antarmuka *React.js* melalui *Inertia.js*. Kontrak pintar PemiraUHO.sol dikompilasi menggunakan compiler *Solidity* versi 0.8.20 dan disebarkan ke jaringan uji coba publik *Ethereum Sepolia Testnet*. Modul Gasless *Relayer* dieksekusi melalui pustaka *Ethers.js* v6 dengan memanfaatkan akun perantara sistem KPU-M terpusat. Alur pemungutan suara berlangsung transparan: pemilih melakukan login dengan NIM dan kata sandi, membuka bilik suara digital, memilih kartu pasangan calon, lalu menekan tombol konfirmasi ganda. *Backend Laravel* menyusun berkas *payload JSON* suara, menambahkan *cryptographic salt* 32-byte acak berkekuatan 256-bit, menghitung nilai *hash* SHA-256, dan mengeksekusi fungsi rekamSuara pada *smart contract* PemiraUHO.sol melalui perantara Gasless *Relayer*. Berdasarkan pengujian terhadap 10 transaksi berturut-turut pada *Sepolia Testnet*, transaksi berhasil divalidasi dan ditambang (*mined*) ke dalam blok jaringan uji dalam kurun waktu rata-rata 12,4 detik tanpa memotong saldo dompet kripto pemilih. Waktu konfirmasi ini diukur secara presisi dari saat modul *relayer* memanggil fungsi *sendTransaction*() hingga diterbitkannya bukti tanda terima blok (transaction receipt). Meskipun waktu 12,4 detik sangat memadai untuk pengujian di jaringan uji coba, perlu dinyatakan secara objektif bahwa kapasitas *throughput* sistem dalam menangani beban pemungutan suara serentak (*stress test* / concurrent peak load) pada skala puluhan ribu mahasiswa UHO belum diukur dalam penelitian ini dan direkomendasikan sebagai fokus kajian pengembangan lanjutan.

3.2. Pengujian Fungsionalitas Sistem (*Black Box* Testing)

Pengujian fungsionalitas sistem dievaluasi melalui 10 skenario uji kasus menggunakan teknik *Black Box* Testing *Boundary Value Analysis*. Tujuan pengujian adalah memverifikasi kesesuaian

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

eksekusi antarmuka, pembatasan hak pilih, penanganan serangan pemilih ganda, dan kepatuhan eksekusi *smart contract*. Rangkuman hasil pengujian fungsionalitas disajikan pada Tabel 2.

Tabel 2. Hasil Pengujian Fungsional Sistem Menggunakan *Black Box* Testing

No.	Skenario Pengujian	Masukan yang Diberikan	Hasil yang Diharapkan	Hasil Pengujian	Status
1	Autentikasi Mahasiswa Valid	NIM dan Password SIAKAD terdaftar	Sistem mengizinkan masuk ke bilik suara	Berhasil masuk ke dashboard pemilih	Valid
2	Autentikasi Kredensial Salah	NIM benar, Password salah	Sistem menolak akses dan menampilkan error	Akses ditolak, pesan peringatan muncul	Valid
3	Pengecekan DPT Status Non-Aktif	Akun mahasiswa non-aktif / cuti	Sistem memblokir hak suara	Hak akses bilik suara dinonaktifkan	Valid
4	Pemilihan Kandidat Presma	Klik tombol Pilih pada Paslon	Muncul dialog konfirmasi pilihan paslon	Dialog modal konfirmasi terbuka	Valid
5	Batal Pilihan pada Modal	Klik tombol Batal pada konfirmasi	Dialog tertutup, suara belum terkirim	Kembali ke bilik suara tanpa mutasi	Valid
6	Konfirmasi Final Pencoblosan	Klik tombol Ya, Kirim Suara	*Relayer* mengeksekusi on-chain, terbit receipt	Transaksi on-chain sukses, receipt terbit	Valid
7	Penolakan *Hash* Suara yang Sudah Tercatat	Masukan *hash* identik yang telah terekam on-chain	*Smart contract* memicu revert 'Suara Sudah Digunakan'	Transaksi ditolak on-chain, status reverted	Valid
8	Pencegahan Pencoblosan Ganda	Login ulang akun yang telah memilih	Sistem mengunci bilik suara dan menampilkan receipt	Bilik suara terkunci permanen	Valid
9	Verifikasi Tanda Terima Digital	Akses menu verifikasi mandiri	Sistem menampilkan detail *hash* dan link *Sepolia*	Data *hash* dan link *Etherscan* tampil	Valid
10	Rekapitulasi Suara Real-Time	Akses dasbor KPU-M	Sistem menampilkan agregasi suara on-chain valid	Perolehan suara teragregasi sinkron	Valid

Hasil pengujian pada Tabel 2 menunjukkan tingkat keberhasilan fungsionalitas 100% di mana 10 dari 10 skenario uji berjalan sesuai rancangan. Secara khusus, pada skenario ke-7 yang menguji 'Penolakan *Hash* Suara yang Sudah Tercatat', sistem secara tegas menolak masukan *hash* identik yang telah terekam pada *smart contract*, di mana transaksi digagalkan melalui mekanisme revert otomatis. Klaim penegakan prinsip satu mahasiswa satu suara didukung oleh evaluasi pemeriksaan berlapis: pada lapisan off-chain, status pemilih langsung ditandai has_voted = true dan *session token* dikunci, sedangkan pada lapisan on-chain, *mapping* hasVoted[voterHash] pada *smart contract* memvalidasi bahwa tidak ada satu pun identitas kriptografis yang dapat mencoblos lebih dari satu kali.

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

3.3. Pengujian Kinerja Algoritma Kriptografi SHA-256

Pengujian kriptografi SHA-256 dievaluasi untuk membuktikan dua karakteristik fundamental: sifat deterministik mutlak dan tingkat keacakan difusi bit melalui pengukuran efek longsoran (*Avalanche Effect*). Sifat deterministik dibuktikan dengan menguji lima sampel masukan data pemira yang di-*hash* dua kali pada waktu berbeda; seluruh pasangan *hash* menghasilkan nilai heksadesimal yang 100% identik. Selanjutnya, pengujian *Avalanche Effect* dilakukan dengan menyimulasikan lima skenario mutasi data minimal dan mengukur jumlah bit keluaran yang mengalami pembalikan (*bit flipping*) dari total 256 bit *digest*. Rincian hasil pengujian dilaporkan pada Tabel 3.

Tabel 3. Hasil Pengujian Efek Longsoran (*Avalanche Effect*) SHA-256

No.	Entitas Data Masukan	Karakteristik Mutasi Masukan	Bit Berubah (D)	Total Bit (N)	*Avalanche Effect* (%)
1	*Payload* Suara Pemilih	Perubahan nomor paslon candidate_id (1 digit)	134	256	52,34%
2	Stempel Waktu Pemilihan	Pergeseran timestamp sebesar 1 detik	129	256	50,39%
3	Garam Kriptografis (*Salt*)	Mutasi 1 karakter pada representasi byte *salt*	138	256	53,91%
4	Format Teks *JSON*	Penyisipan 1 karakter spasi (mengubah panjang)	131	256	51,17%
5	UUID Transaksi Suara	Perubahan 1 karakter heksadesimal pada UUID	136	256	53,13%
Rata-rata	-	Rata-rata perubahan bit dari lima skenario uji	133,6	256	52,19%

Berdasarkan data pada Tabel 3, pengubahan minimal satu digit pada candidate_id menghasilkan pembalikan sebanyak 134 bit dari total 256 bit keluaran (52,34%). Pergeseran waktu 1 detik membalikkan 129 bit (50,39%), mutasi satu karakter *salt* membalikkan 138 bit (53,91%), penyisipan satu karakter spasi yang mengubah panjang masukan membalikkan 131 bit (51,17%), dan modifikasi satu digit UUID membalikkan 136 bit (53,13%). Dari kelima percobaan tersebut, diperoleh rata-rata perubahan bit sebesar 52,19%. Nilai ini diinterpretasikan sebagai hasil acak yang berfluktuasi secara ideal di sekitar nilai acuan teoretis 50% (di mana 50% merepresentasikan tingkat keacakan independen sempurna dari setiap bit keluaran). Hasil ini membuktikan bahwa algoritma SHA-256 pada sistem yang dikembangkan memiliki sifat difusi kriptografis yang sangat tinggi sehingga perubahan sekecil apa pun pada data suara akan mengubah intisari *hash* secara radikal.

3.4. Pengujian Integritas Data dan Audit On-Chain *Blockchain*

Pengujian integritas data dirancang untuk memvalidasi kemampuan sistem dalam membuktikan terjadinya manipulasi data lokal melalui pencocokan catatan off-chain terhadap catatan kekal pada *smart contract Sepolia*. Simulasi pengujian dibatasi secara ketat pada empat skenario manipulasi data dan satu catatan pembanding normal yang valid. Hasil pengujian disajikan pada Tabel 4.

Hasil pengujian pada Tabel 4 membuktikan bahwa sistem audit hibrida berhasil mendeteksi empat dari empat kasus manipulasi basis data lokal secara deterministik (100%), sementara satu catatan normal terverifikasi valid secara konsisten. Keberhasilan ini dimungkinkan karena *smart contract* PemiraUHO.sol memancarkan log event VoteCast(uint256 indexed candidateId, bytes32 voteHash, uint256 timestamp) pada buku besar terdistribusi *Sepolia* setiap kali transaksi berhasil dieksekusi. Di sisi pemilih, tanda terima digital (*digital vote receipt*) yang diterbitkan memuat informasi penting berupa *Transaction Hash Sepolia*, stempel waktu, dan nilai vote_hash SHA-256. Melalui informasi pada tanda terima tersebut, mahasiswa dapat melakukan verifikasi mandiri (*individual verifiability*) dengan memeriksa ketercantuman transaksi pada penjelajah blok *Etherscan* tanpa harus mengekspos pilihan politiknya kepada publik, karena pilihan suara telah terkunci secara matematis di dalam *digest* SHA-256 yang diperkuat *salt* 32-byte. Dengan demikian, sistem berhasil menyeimbangkan dua tuntutan yang

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

saling bertolak belakang: asas Rahasia bagi pemilih dan asas Terbuka/Jujur bagi proses audit perolehan suara.

Tabel 4. Hasil Pengujian Integritas Data Melalui Audit *Blockchain*

Skenario Uji Audit	Manipulasi Data yang Disimulasikan	Nilai *Hash* Lokal (Off-Chain)	Nilai *Hash Sepolia* (On-Chain)	Status Integritas
Kasus Normal (Valid)	Tidak ada modifikasi (suara murni pemilih)	0x7f83b1657ff1... (Identik)	0x7f83b1657ff1... (Identik)	VALID (Data Konsisten)
Manipulasi Paslon	Admin mengubah candidate_id 1 menjadi 2 di DB	0x9c3d4f8e12a0... (Berubah)	0x7f83b1657ff1... (Tetap)	ANOMALI (Manipulasi Terdeteksi)
Manipulasi Nilai *Hash*	Admin merekayasa kolom vote_hash di DB	0x112233445566... (Palsu)	0x7f83b1657ff1... (Tetap)	ANOMALI (Manipulasi Terdeteksi)
Manipulasi *Token* Audit	Modifikasi nilai *salt* dan *payload* suara di DB	0xbb88aa224411... (Berubah)	0x7f83b1657ff1... (Tetap)	ANOMALI (Manipulasi Terdeteksi)
Injeksi Suara Ilegal	Penyisipan baris rekaman baru tanpa *relayer*	Record ada di database *MySQL*	*Hash* tidak terdaftar di *Sepolia*	ANOMALI (Suara Palsu Ditolak)

3.5. Evaluasi Penerimaan Pengguna (*User Acceptance Testing*)

Evaluasi penerimaan pengguna akhir diukur menggunakan pengujian *User Acceptance Testing* (UAT) yang melibatkan 10 responden pemangku kepentingan PEMIRA UHO (satu administrator KPU-M, dua saksi paslon, dan tujuh mahasiswa pemilih perwakilan tujuh fakultas) terhadap 10 butir instrumen kuesioner terstruktur (P1–P10). Tabulasi distribusi penilaian responden disajikan pada Tabel 5.

Berdasarkan data tabulasi pada Tabel 5, total skor aktual yang diperoleh dari 10 responden terhadap 10 butir pernyataan kuesioner adalah sebesar 442 dari total skor maksimal ideal teoretis sebesar 500 (10 responden x 10 butir pertanyaan x skor maksimal 5). Melalui Persamaan (6), diperoleh persentase kelayakan akhir sebesar 88,40%. Merujuk pada kriteria interpretasi skor kelayakan sistem menurut Sugiyono (2019), persentase kelayakan sebesar 88,40% berada pada rentang 81%–100% yang secara definitif mengklasifikasikan sistem *e-voting* terdesentralisasi ini ke dalam kategori 'Sangat Layak' untuk diterapkan. Butir P10 memperoleh skor tertinggi sebesar 4,60 (92,0%), yang merefleksikan dukungan penuh dari seluruh responden agar sistem ini diadopsi secara resmi pada PEMIRA UHO. Butir P7 dan P9 masing-masing meraih skor 4,50 (90,0%), membuktikan bahwa integrasi Gasless *Relayer* Pattern berhasil meniadakan resistensi teknis mahasiswa, sedangkan butir transparansi dan keamanan (P5, P6, P8) mencatat skor rata-rata di atas 86,0%, membuktikan bahwa kekhawatiran krisis kepercayaan pemilih sebagaimana diidentifikasi dalam temuan Mubbaraq dkk. (2024) berhasil dijawab melalui arsitektur *blockchain* dan tanda terima digital yang diajukan.

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Tabel 5. Hasil Tabulasi Penilaian Pengujian *User Acceptance Testing* (UAT)

Kode	Indikator Evaluasi UAT	SS (5)	S (4)	CS (3)	TS (2)	STS (1)	Total Skor	Kelayakan (%)
P1	Kebersihan dan Kerapian Tata Letak Antarmuka	4	5	1	0	0	43	86,0%
P2	Kecepatan dan Keandalan Autentikasi Login	4	6	0	0	0	44	88,0%
P3	Kejelasan Profil Paslon dan Visi-Misi	4	6	0	0	0	44	88,0%
P4	Kepraktisan Bilik Suara dan Dialog Konfirmasi	5	4	1	0	0	44	88,0%
P5	Rasa Aman dan Kepastian dari Tanda Terima Digital	4	6	0	0	0	44	88,0%
P6	Kemudahan Memantau Status via *Etherscan Sepolia*	5	4	1	0	0	44	88,0%
P7	Efektivitas Waktu Dibanding Pemilu Kertas	5	5	0	0	0	45	90,0%
P8	Kepercayaan Integritas Suara Berkat SHA-256	4	5	1	0	0	43	86,0%
P9	Kenyamanan Transaksi Bebas Biaya (Gasless *Relayer*)	5	5	0	0	0	45	90,0%
P10	Dukungan Penuh Penerapan Sistem pada PEMIRA UHO	6	4	0	0	0	46	92,0%
Total	Akumulasi Skor Pengujian UAT (10 Responden)	-	-	-	-	-	442	88,40%

4. KESIMPULAN

Penelitian ini telah berhasil mengembangkan dan menguji sistem pemungutan suara elektronik terdesentralisasi berbasis *blockchain Ethereum Sepolia* dan *smart contract* untuk verifikasi suara pada Pemilihan Presiden Mahasiswa Universitas Halu Oleo. Berdasarkan hasil evaluasi yang diperoleh, dapat ditarik simpulan yang terukur: (1) Pengujian fungsionalitas *Black Box* membuktikan bahwa 10 dari 10 skenario fungsional berjalan 100% sesuai harapan, termasuk keberhasilan penolakan terhadap upaya pemilihan ganda dan *hash* suara yang telah tercatat. (2) Pengujian kinerja kriptografi SHA-256 menghasilkan sifat deterministik sempurna dan rata-rata efek longsoran (*avalanche effect*) sebesar 52,19% dari lima skenario mutasi bit masukan, yang berfluktuasi ideal di sekitar nilai acuan teoretis 50%. (3) Pengujian audit integritas data membuktikan sistem mampu mendeteksi empat dari empat kasus manipulasi data lokal secara deterministik (100%) melalui rekonsiliasi catatan lokal terhadap log event *smart contract* di jaringan uji *Sepolia*. (4) Evaluasi *User Acceptance Testing* (UAT) menghasilkan persentase kelayakan akhir sebesar 88,40% dalam kategori 'Sangat Layak' berdasarkan penilaian 10 responden pemangku kepentingan PEMIRA UHO. Simpulan tentang verifikasi mandiri dibatasi secara tegas pada kemampuan pemilih dalam memeriksa status pencatatan transaksi pada buku besar *Sepolia* melalui tanda terima digital tanpa membocorkan pilihan politik rahasia pemilih. Untuk penelitian di masa mendatang, disarankan melakukan pengujian beban serentak (stress testing) berskala masif guna mengukur kapasitas *throughput* transaksi saat melayani puluhan ribu pemilih secara bersamaan.

DAFTAR PUSTAKA

Al-Saegh, A. A., & Al-Hakeem, M. S. (2023). Review study of *e-voting* system based on smart contracts using *blockchain* technology. Iraqi Journal of Science, 64(4), 2001–2022. https://doi.org/10.24996/ijs.2023.64.4.34

Ananda, S., Surya, I. B. K., & Wibowo, H. (2024). The urgency of implementing a *blockchain*-based *e-voting* system in organizing general elections in Indonesia. Research Review International Journal of Multidisciplinary, 9(4), 104–110. https://doi.org/10.31305/rrijm.2024.v09.n04.014

Antonopoulos, A. M., & Wood, G. (2018). Mastering *Ethereum*: Building smart contracts and *DApps*. O'Reilly Media.

Arianto, E., Umam, C., & Handoko, L. B. (2021). Purwarupa sistem pemilihan umum elektronik dengan pemanfaatan protokol *Ethereum* pada teknologi *blockchain*. Transformatika: Jurnal Sains dan Teknologi, 19(1), 88–97. https://doi.org/10.26623/transformatika.v19i1.3060

Aripin, D. W., & Muttaqin, H. F. (2025). Application of *blockchain* technology for *e-voting* systems using smart contracts. Jurnal Indonesia Sosial Teknologi, 6(5), 1845–1856. https://doi.org/10.59141/jist.v6i5.1092

Bashir, I. (2020). Mastering *blockchain*: A deep dive into distributed ledgers, consensus protocols, and smart contracts (3rd ed.). Packt Publishing.

Buterin, V. (2014). A next-generation *smart contract* and *decentralized application* platform. *Ethereum* White Paper, 1–36.

Kalyani, B. J. D., Modadugu, J. K., & Neelima, S. (2025). *Blockchain*-based decentralized voting system with SHA-256 algorithm and facial recognition. International Journal of Reconfigurable and Embedded Systems (IJRES), 14(2), 481–489. https://doi.org/10.11591/ijres.v14.i2.pp481-489

Kelarno, H. A. T., & Widayat, W. (2024). *Smart contract* implementation on *e-voting* system for secure and transparent student election. JNTETI (Jurnal Nasional Teknik Elektro dan Teknologi Informasi UGM), 13(3), 218–227. https://doi.org/10.22146/jnteti.v13i3.10787

Latif, S., Idrees, Z., Ahmad, J., Zheng, L., & Zou, Z. (2022). A systematic literature review and meta-analysis on scalable *blockchain*-based electronic voting systems. Sensors, 22(19), Article 7585. https://doi.org/10.3390/s22197585

Mubbaraq, F. R., Ransi, N., & Hamundu, F. M. (2024). Analisis penggunaan aplikasi *e-voting* PEMIRA Universitas Halu Oleo: Perluasan *Technology Acceptance Model* dengan *Trust in Internet* sebagai variabel moderator. AnoaTIK: Jurnal Teknologi Informasi dan Komputer, 2(2), 94–100. https://doi.org/10.33772/anoatik.v2i2.72

Mustaqbal, M. S., Firdaus, R. F., & Rahmadi, H. (2015). Pengujian aplikasi menggunakan *black box* testing *boundary value analysis* (studi kasus: aplikasi prediksi kelulusan SNMPTN). Jurnal Ilmiah Teknologi Informasi Terapan (JITTER), 1(3), 31–36. https://doi.org/10.33197/jitter.vol1.iss3.2015.60

Nakamoto, S. (2008). Bitcoin: A *peer-to-peer* electronic cash system. Decentralized Business Review, 1–9.

National Institute of Standards and Technology (NIST). (2015). Secure *Hash* Standard (SHS) (FIPS PUB 180-4). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.180-4

Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: From Internet voting to *blockchain* voting. Journal of Cybersecurity, 7(1), Article tyaa025. https://doi.org/10.1093/cybsec/tyaa025

Pressman, R. S., & Maxim, B. R. (2020). Software engineering: A practitioner's approach (9th ed.). McGraw-Hill Education.

Sadia, K., Masuduzzaman, M., Paul, R. K., & Islam, A. (2019). *Blockchain* based secured *e-voting* by using the assistance of *smart contract*. arXiv preprint arXiv:1910.13635, 1–8. https://doi.org/10.48550/arXiv.1910.13635

Sommerville, I. (2016). Software engineering (10th ed.). Pearson Education.

Sugiyono. (2019). Metode penelitian kuantitatif, kualitatif, dan R&D (Edisi ke-2). Alfabeta.

Tas, R., & Tanriöver, Ö. (2020). A systematic review of challenges and opportunities of *blockchain* for *e-voting*. Symmetry, 12(8), Article 1328. https://doi.org/10.3390/sym12081328

DOI: https://doi.org/10.54082/jupin.2964
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Tedyyana, A., Ghazali, O., Asnafi, T., Purbo, O. W., Harun, N. Z., & Riza, F. (2024). Transforming the voting process integrating *blockchain* into *e-voting* for enhanced transparency and security. TELKOMNIKA (Telecommunication Computing Electronics and Control), 22(2), 311–320. https://doi.org/10.12928/telkomnika.v22i2.25368

Universitas Halu Oleo. (2023). Peraturan Rektor Universitas Halu Oleo Nomor 1 Tahun 2023 tentang pedoman tata kelola organisasi kemahasiswaan dan tata cara Pemilihan Raya Mahasiswa (PEMIRA) di lingkungan Universitas Halu Oleo. Universitas Halu Oleo.