JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1903- 1911
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/ 10.62712/juktisi.v4i3.782

Implementasi Blockchain Menggunakan Multi-Signature Approval dan Merkle Tree untuk Sistem E-Voting Pemilu

Villeneuve Andhira Suwandhi[1,*], Yudi Wibisono[2], Rizky Rahman[3]

[1,2,3] Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Ilmu Komputer, Universitas Pendidikan Indonesia, Bandung, Indonesia
Email: [1*]v.andhira@upi.edu, [2]yudi@upi.edu, [3]rizky_rjp@upi.edu
(* Email Corresponding Author: v.andhira@upi.edu)
Received: January 8, 2026 | Revision: January 10, 2026 | Accepted: January 10, 2026

Abstrak

Pelaksanaan pemilihan umum konvensional di Indonesia masih menghadapi tantangan besar terkait tingginya biaya logistik, risiko manipulasi data, dan kurangnya transparansi proses yang memicu ketidakpercayaan publik. Penelitian ini bertujuan untuk merancang purwarupa sistem *e-voting* masa depan dengan mengusulkan *Hybrid Voting Framework* berbasis teknologi *blockchain Ethereum* dan *InterPlanetary File System (*IPFS). Masalah skalabilitas dan privasi diselesaikan melalui integrasi struktur data *Merkle Tree*, di mana hanya nilai *root* sebesar 32-bytes yang disimpan secara *on-chain*, sementara data sensitif dikelola secara *off-chain*. Untuk memitigasi risiko sentralisasi otoritas, sistem ini menerapkan konsep mekanisme konsensus *Proof of Authority* (PoA) dengan skema *multi-signature approval* yang mewajibkan persetujuan mayoritas *validator* (>50%) pada setiap aksi administratif. Hasil pengujian menunjukkan bahwa sistem mampu menjaga integritas suara melalui prinsip *one person one vote* dengan waktu pembuatan blok yang stabil di bawah 10 detik. Selain itu, fitur *Recent Activity Log* dan *Verify My Vote* berhasil menyajikan transparansi *real-time* dengan memanfaatkan *event logs* dari *smart contract*. Secara keseluruhan, purwarupa ini membuktikan bahwa penggunaan *blockchain* dapat menciptakan sistem pemungutan suara yang aman, akuntabel, dan efisien, sekaligus memberikan perlindungan privasi yang maksimal bagi pemilih melalui pembuktian kriptografi yang kuat.

Kata Kunci: *Blockchain*, *E-voting*, *Merkle Tree*, *Multi-signature Approval*, *Smart Contract*, Transparansi.

Abstract

The implementation of conventional general elections in Indonesia still faces significant challenges, including high logistical costs, risks of data manipulation, and a lack of process transparency, which triggers public distrust. This research aims to design a future e-voting system prototype by proposing a Hybrid Voting Framework based on Ethereum blockchain technology and the InterPlanetary File System (IPFS). Scalability and privacy issues are addressed through the integration of the Merkle Tree data structure, where only a 32-byte root value is stored on-chain, while sensitive data is managed off-chain. To mitigate the risk of authority centralization, the system implements a concept from Proof of Authority (PoA) consensus mechanism with a multi-signature approval scheme, requiring the consensus of the majority of validators (>50%) for every administrative action. The test results show that the system is capable of maintaining voting integrity through the one-person-one-vote principle with a stable block creation time of under 10 seconds. Furthermore, the Recent Activity Log and "Verify My Vote" features successfully provide real-time transparency by utilizing event logs from smart contracts. Overall, this prototype proves that the use of blockchain can create a secure, accountable, and efficient voting system, while simultaneously providing maximum privacy protection for voters through robust cryptographic proof.

Keywords*: Blockchain, E-voting, Merkle Tree, Multi-signature Approval, Smart Contract, Transparency.*

1. PENDAHULUAN

Pemilihan umum (pemilu) merupakan instrumen utama dalam sistem demokrasi yang berfungsi sebagai sarana kedaulatan rakyat untuk memilih pemimpin guna mencapai tujuan masyarakat yang adil dan makmur. Di Indonesia, pelaksanaan pemilu masih didominasi oleh metode konvensional berbasis kertas. Meskipun dianggap paling akomodatif, metode pencoblosan kertas ini masih memiliki sejumlah kelemahan fundamental. Permasalahan yang sering muncul meliputi tingginya biaya logistik, kerentanan terhadap kesalahan manusia dalam proses perhitungan, potensi manipulasi suara, hingga keterlambatan pengumuman hasil akhir dapat memicu ketidakpercayaan publik [1]. Implementasi teknologi menggunakan *e-voting*, yaitu digitalisasi seluruh prosedur pemilu, menawarkan proses yang cepat dan penghematan sumber daya sebagai solusi permasalahan pada pemilu konvensional. Namun, implementasinya secara luas masih terhambat oleh pemalsuan dan perubahan data jika tidak dikelola dengan teknologi keamanan dengan tepat yang transparansi prosesnya masih dipertanyakan [2].

Teknologi *blockchain* hadir sebagai solusi baru yang menawarkan keamanan melalui sistem pencatatan data terdesentralisasi dan bersifat *immutable* atau tidak dapat diubah. Karakteristik utama *blockchain* seperti transparansi, auditabilitas, dan ketahanan terhadap serangan titik tunggal (*single point of failure*) menjadikannya sebagai teknologi yang ideal untuk sistem *e-voting* [2], [3], [4]. Akan tetapi, implementasi *blockchain* dalam sistem *e-voting* untuk pemilu masih menghadapi tantangan dan risiko yang kompleks. Dari sisi keamanan dan privasi, sifat data yang *immutable* sering kali berbenturan dengan regulasi perlindungan data terkait hak penghapusan identitas pemilih, di samping adanya risiko kerentanan enkripsi di masa depan seiring kemajuan kekuatan komputasi [5]. Secara teknis, kendala utama terletak pada aspek skalabilitas dan tingginya konsumsi energi pada jaringan luas. Tantangan lain yang

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1903- 1911
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/ 10.62712/juktisi.v4i3.782

tidak kalah penting adalah kompleksitas integrasi dengan sistem infrastruktur lama yang memerlukan biaya tinggi serta penyesuaian regulasi yang mampu melegitimasi penggunaan solusi berbasis *blockchain* secara nasional [6], [7].

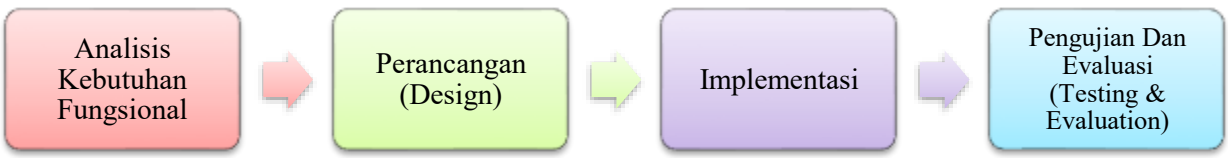
Tinjauan terhadap penelitian literatur dalam lima tahun terakhir menunjukkan adanya perkembangan signifikan dalam integrasi teknologi *blockchain* yang menjadi fondasi utama dalam mengidentifikasi celah riset pada penelitian ini. Pertama, penggunaan *enterprise blockchain* berbasis *Hyperledger Fabric* untuk mencapai skalabilitas tinggi, namun sistem ini memiliki ketergantungan pada infrastruktur *Membership Service Provider* (MSP) yang kompleks dan memerlukan sumber daya komputasi yang besar untuk mengelola identitas terpusat [8]. Kedua, potensi penggunaan *smart contract* dan *DApps* pada jaringan *Ethereum* publik, namun mencatat adanya hambatan besar berupa tingginya biaya *gas fee* dan keterbatasan skalabilitas (12-20 transaksi per detik) pada mekanisme *Proof of Work* (PoW) sebelum transisi penuh ke *Ethereum 2.0* [9]. Ketiga, sistem *e-voting* pada jaringan *private blockchain* dengan algoritma konsensus PBFT untuk memitigasi risiko manipulasi data oleh administrator pusat dan mempercepat waktu pemrosesan transaksi hingga 1.500 TPS, meskipun penggunaan jaringan privat murni tersebut memiliki keterbatasan dalam hal transparansi publik yang bersifat terbuka [2]. Keempat, sistem PVPBC yang mengintegrasikan protokol *Selene* pada *permissioned blockchain* untuk menjamin verifikasi hasil pilihan secara *plaintext* oleh pemilih, namun sistem ini memiliki ketergantungan pada pihak ketiga terpercaya untuk mengelola *token* identitas, serta menunjukkan latensi rata-rata sebesar 6,275 detik yang cenderung meningkat secara linear seiring bertambahnya jumlah kandidat [10]. Kelima, integrasi *Homomorphic Encryption* (HE) untuk mengenkripsi data demografis pemilih, sehingga memungkinkan analisis statistik hasil pemilu tanpa melanggar privasi, namun implementasi HE ini menuntut kapasitas penyimpanan data yang besar dan memiliki kompleksitas tinggi dalam menjaga kecepatan komputasi pada skala data massal [11]. Keenam, kerangka kerja DAO-FL yang memanfaatkan *smart contract* dan mekanisme *multi-signature* untuk verifikasi *input-output* yang terdesentralisasi, namun arsitektur ini memiliki kendala pada biaya transaksi yang tinggi akibat mekanisme *on-chain voting* serta latensi yang tidak menentu yang membatasi efektivitasnya pada aplikasi bersifat *real-time* [12]. Ketujuh, integrasi arsitektur *Merkle Patricia Tree* dari *Ethereum* dengan algoritma CP-ABE dan *Homomorphic Encryption* untuk menciptakan sistem keamanan berlapis pada lingkungan *cloud multi-tenant*, yang berhasil mencapai tingkat keberhasilan verifikasi silang sebesar 90-91,5% namun memerlukan manajemen kunci yang sangat kompleks pada delapan tahapan komunikasi antar *tenant* [13]. Kedelapan, sistem penyimpanan data kendaraan yang mengombinasikan *Ethereum* dan IPFS untuk efisiensi penyimpanan data besar, serta mengimplementasikan fitur pencarian berbasis kata kunci (*keyword search*) melalui filter *log* kejadian *smart contract* menggunakan pustaka *Ethers.js* [14]. Kesembilan, kerangka kerja konseptual berbasis IPFS dan *smart contract Ethereum* yang menggunakan algoritma enkripsi homomorfik ringan berbasis koefisien binomial untuk mencegah pemalsuan ijazah akademik, dengan hasil analisis yang menunjukkan ketahanan terhadap serangan *brute force* dan *Sybil attack* [15].

Secara keseluruhan, literatur saat ini masih menyisakan tantangan besar dalam menyeimbangkan antara transparansi publik, efisiensi penyimpanan identitas, dan kecepatan transaksi tanpa biaya tinggi. Berdasarkan analisis GAP tersebut, penelitian ini mengusulkan sebuah *Hybrid Voting Framework*. Keterbaharuan yang ditawarkan terletak pada integrasi struktur data *Merkle Tree* untuk memvalidasi hak pilih secara *on-chain* dengan beban memori minimal, serta penggunaan konsep mekanisme konsensus *Proof of Authority* (PoA) yang melibatkan *validator* untuk mencegah kekuasaan terpusat. Tujuan utama dari penelitian ini adalah merancang dan membangun purwarupa sistem *e-voting* berbasis *blockchain* yang tidak hanya menjamin keamanan dan transparansi, tetapi juga memiliki efisiensi terhadap penyimpanan data identitas sensitif secara *off-chain* atau diluar rantai *blockchain*. Harapannya, sistem purwarupa ini dapat memberikan model teknologi yang andal bagi instansi penyelenggara pemilu untuk meningkatkan kualitas demokrasi digital yang aman, transparan, dan akuntabel.

2. METODOLOGI PENELITIAN

2.1 Kerangka Kerja Penelitian

Penelitian ini menggunakan pendekatan *System Development Life Cycle* (SDLC) dengan model *Waterfall*. Prosedur penelitian dilakukan secara bertahap dan sistematis sebagai berikut:



Gambar 1. Tahapan Penelitian

a. Analisis Kebutuhan (*Requirement Analysis*)
Tahap ini mengidentifikasi terhadap spesifikasi yang diperlukan agar sistem *e-voting* berbasis *blockchain* dapat berjalan optimal.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1903- 1911
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/ 10.62712/juktisi.v4i3.782

1. Identifikasi Kebutuhan Fungsional (F): Memetakan fitur utama seperti hak akses otoritas (admin), manajemen kandidat, registrasi data pemilih terdaftar dengan *merkle root* dan IPFS, serta mekanisme *one person one vote*. Fokusnya adalah memastikan alur teknis pemungutan suara dan *multi-signature* tervalidasi dengan benar.
2. Identifikasi Kebutuhan Non-Fungsional (NF): Menentukan standar kualitas sistem yang meliputi aspek keamanan, kinerja, privasi, serta transparansi agar *ledger* dapat diaudit oleh publik.

b. Perancangan (*Design*)
Tahap ini merupakan proses perancangan dari kebutuhan ke dalam arsitektur purwarupa sistem sebelum direalisasikan. Merancang arsitektur jaringan tipe *Permissioned Public* (*Hybrid*) *Blockchain* mandiri untuk mengatasi kendala biaya dan skalabilitas, menyusun logika pemrograman menggunakan *Solidity* secara modular agar mudah pengembangannya, dan model kriptografi dengan mengintegrasikan struktur data *Merkle Tree* untuk efisiensi penyimpanan data pemilih serta penerapan *hashing off-chain* untuk menjaga kerahasiaan identitas (pseudonimitas).

c. Implementasi (*Implementation*)
Tahap ini merupakan proses merealisasikan pada rancangan purwarupa sistem. Teknisnya menggunakan jaringan lokal *Ethereum* pada *Ganache* dan melakukan *deployment* kontrak menggunakan *framework Hardhat*. Pengembangan antarmuka menggunakan *React.js* dan menghubungkan dengan *blockchain* menggunakan pustaka *Ethers.js* serta *MetaMask* sebagai layanan otorisasi transaksi bagi pengguna.

d. Pengujian dan Evaluasi (*Testing & Evaluation*)
Sistem yang telah dikembangkan diuji menggunakan dua metode utama untuk memastikan tidak ada celah kemanan atau kesalahan logika dan memenuhi kebutuhan yang telah didefinisikan. Metode pertama, *white-box testing* yang melakukan audit terhadap baris kode di dalam *smart contract* untuk memastikan fungsi-fungsi berjalan sesuai logika yang diharapkan tanpa *bug* dan *error*. Kedua, metode *black-box testing* yang menguji fungsionalitas sistem dari sisi pengguna antarmuka untuk memastikan alur proses pemilu dari awal pendaftaran, pemungutan suara, hingga perhitungan suara dapat dilakukan dengan mudah tanpa harus memahami teknis di baliknya. Kemudian, hasil pengujian dianalisis kembali terhadap parameter keberhasilan yang telah ditetapkan untuk memeriksa apakah target hasil yang diinginkan sudah tercapai dan memastikan bahwa sistem telah memenuhi standar sehingga siap direkomendasikan sebagai solusi *e-voting* yang aman, transparan, dan akuntabel.

2.2 Analisis Kebutuhan (*Requirement Analysis*)

Analisis kebutuhan dilakukan untuk memetakan spesifikasi sistem *e-voting* berbasis *blockchain*. Kebutuhannya dibagi menjadi dua kategori utama, yaitu fungsional (F) dan non-fungsional (NF):

a. Kebutuhan Fungsional (F)
Sistem berfokus pada tiga pilar utama: administrasi pemilu, pemungutan suara, dan mekanisme konsensus. Pada sisi administrasi, otoritas (admin) memiliki hak penuh untuk mengelola periode pemilu (F1.1), mendaftarkan kandidat (F1.3), dan menambahkan *validator* untuk keperluan validasi (F1.4). Otoritas juga bertanggung jawab meregistrasi data pemilih melalui struktur *Merkle Root* yang referensi data lengkapnya disimpan pada IPFS (F1.2). Dalam proses pemungutan suara, sistem mewajibkan verifikasi identitas pemilih menggunakan kredensial *off-chain* IPFS (F2.1) dan pengiriman *Merkle Proof* guna menjamin anonimitas tanpa menghilangkan hak pilih (F2.2). Integritas suara dijaga ketat melalui prinsip *one person one vote* guna memastikan setiap akun hanya dapat memberikan suara satu kali per periode (F2.3), diikuti dengan tampilan konfirmasi pencatatan suara ke *blockchain* bagi pemilih (F2.4). Sementara itu, pada level jaringan, *validator* berperan dalam skema *multi-signature* (F3.1) untuk memvalidasi aksi administratif sensitif, serta menggunakan validasi *on-chain* berbasis *Merkle Proof* untuk memastikan keabsahan daftar pemilih tanpa perlu menyimpan data sensitif seperti NIK secara mentah di dalam *ledger* (F3.2).

b. Kebutuhan Non-Fungsional (NF)
Fokus utama kategori ini adalah menjamin kualitas operasional dan keamanan tingkat tinggi. Dari aspek keamanan, sistem memastikan imutabilitas data suara yang telah dicatat (NF1.1), kerahasiaan kunci enkripsi data *off-chain* (NF1.2), dan kontrol akses ketat di mana hanya *wallet* otoritas yang dapat menjalankan fungsi-fungsi sensitif (NF1.3). Aspek kinerja dioptimalkan melalui skalabilitas transaksi yang tinggi (NF2.1) dengan target waktu pembuatan blok di bawah 10 detik (NF2.2), waktu respon suara maksimal 5 detik (NF2.4), serta penggunaan *Merkle Tree* untuk efisiensi biaya transaksi atau *gas fee* (NF2.3). Privasi pemilih dijaga melalui mekanisme anonimitas suara secara individual (NF3.1) dan pseudonimitas identitas di mana identitas asli pemilih hanya dicatat sebagai *Hash ID* samaran (NF3.2). Terakhir, aspek transparansi dan auditabilitas dipenuhi melalui penyediaan *ledger* publik yang dapat diaudit oleh *read-only nodes* secara terbuka (NF4.1) serta penggunaan verifikasi kriptografi yang memeriksa kesesuaian kunci rahasia milik akun pemilih tanpa menyimpan data sensitif di dalam jaringan (NF4.2).

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1903- 1911
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/ 10.62712/juktisi.v4i3.782

2.3 Perancangan (*Design*)

Purwarupa ini menggunakan tipe *Permissioned Public Blockchain* mandiri untuk menghindari masalah skalabilitas pada jaringan publik. Model ini mengintegrasikan *Hybrid Voting Framework* yang menggabungkan *Merkle Tree* untuk data pemilih dan *M-of-N Approval* sebagai bentuk konsep mekanisme konsensus *Proof of Authority* (PoA) untuk tata kelola administrasi. Desain sistem menggunakan *Smart Contract* dengan bahasa pemrograman *Solidity* yang disusun secara modular untuk meningkatkan auditabilitas dan keamanan.
Model keamanan mengandalkan kriptografi:

a. Pseudonimitas Identitas: Melakukan *hashing* identitas secara *off-chain* sehingga data yang tercatat di *blockchain* bersifat unik namun anonim. Hal ini memungkinkan verifikasi tanpa mengungkapkan data pribadi seperti NIK.
b. Efisiensi *Merkle Tree*: Mengimplementasikan *proof* yang hanya menyimpan satu nilai *root* (32-*bytes*) di *blockchain*. Hal ini mereduksi beban penyimpanan dan biaya transaksi (*gas fee*) dibandingkan penyimpanan data pemilih secara mentah pada rantai blok.

2.4 Implementasi (*Implementation*)

Realisasi purwarupa mencakup pembangunan jaringan lokal *Ethereum* menggunakan *Ganache*. Pengembangan logika kontrak dilakukan dengan *framework Hardhat* dan bahasa pemrograman *Solidity* versi ^0.8.0. Untuk antarmuka pengguna, sistem menggunakan *React.js* yang menggunakan pustaka *Ethers.js* sebagai jembatan integrasi. Integrasi ini memungkinkan interaksi langsung antara pengguna dengan *smart contract* melalui ekstensi dompet digital *MetaMask* sebagai alat otorisasi transaksi.

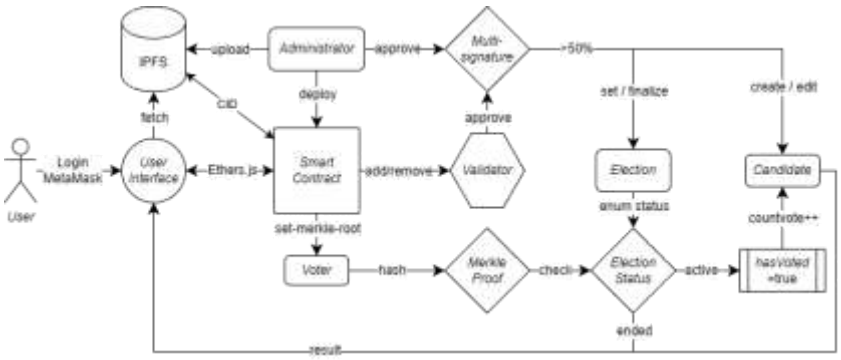
2.5 Pengujian dan Evaluasi (*Testing & Evaluation*)

Strategi pengujian yang digunakan untuk menjamin integritas sistem, yaitu *White-box Testing* yang berfokus pada validasi logika internal *smart contract* dan *Black-box Testing* untuk menguji alur kerja dari perspektif pengguna melalui antarmuka. Sistem dinyatakan berhasil apabila memenuhi kriteria kelulusan pada aspek kebutuhan fungsionalitas melalui uji coba skenario.

3. HASIL DAN PEMBAHASAN

Bagian ini memaparkan hasil dari seluruh rangkaian perancangan, pengembangan, serta pengujian purwarupa sistem *e-voting* berbasis *blockchain* yang telah dilakukan. Fokus utama dari pembahasan ini adalah untuk mengevaluasi efektivitas penggunaan *Hybrid Voting Framework* dalam menjawab tantangan keamanan, transparansi dan efisiensi pada pemilihan umum *online* atau *e-voting*. Pemaparan akan diawali dengan realisasi arsitektur sistem dan implementasi *smart contract* menggunakan bahasa pemrograman *Solidity*, diikuti dengan analisis teknis mengenai integrasi struktur data *Merkle Tree* untuk perlindungan privasi pemilih. Selanjutnya, bagian ini akan mendemonstrasikan konsep mekanisme konsensus *Proof of Authority* (PoA) melalui skema *multi-signature approval* sebagai solusi atas risiko sentralisasi otoritas. Untuk membuktikan kualitas operasional sistem, hasil pengujian fungsionalitas dan performa melalui metode *white-box* dan *black-box testing*. Keseluruhan analisis ini bertujuan untuk memvalidasi bahwa purwarupa yang dikembangkan mampu menciptakan sistem *e-voting* berbasis *blockchain* yang meningkatkan keamanan dan transparansi pada ekosistem demokrasi digital yang *immutable*, akuntabel, dan efisien.

3.1 Arsitektur Purwarupa Sistem dan *Smart Contract*



Gambar 2. Arsitektur Purwarupa Sistem

Gambar 2 menunjukkan arsitektur purwarupa sistem yang mengintegrasikan lapisan antarmuka pengguna, logika bisnis pada rantai blok, dan media penyimpanan terdistribusi. Arsitektur purwarupa sistem ini dirancang menggunakan model *Hybrid Voting Framework* yang secara strategis memisahkan antara beban kerja *on-chain* dan *off-chain* untuk mencapai efisiensi maksimal.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1903- 1911
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/ 10.62712/juktisi.v4i3.782

Dalam arsitektur ini, antarmuka pengguna berbasis *React.js* berkomunikasi dengan jaringan *blockchain* melalui pustaka *Ethers.js*. Peran *smart contract* dalam penelitian ini adalah sebagai *single source of truth* yang mengelola seluruh logika pemilihan secara otomatis tanpa intervensi pihak ketiga. Untuk mengatasi kendala skalabilitas penyimpanan pada *blockchain*, data statis *metadata* pemilih disimpan pada jaringan *InterPlanetary File System* (IPFS). *Smart contract* hanya akan menyimpan referensi berupa *Content Identifier* (CID) yang unik dan bersifat permanen untuk merujuk pada IPFS.

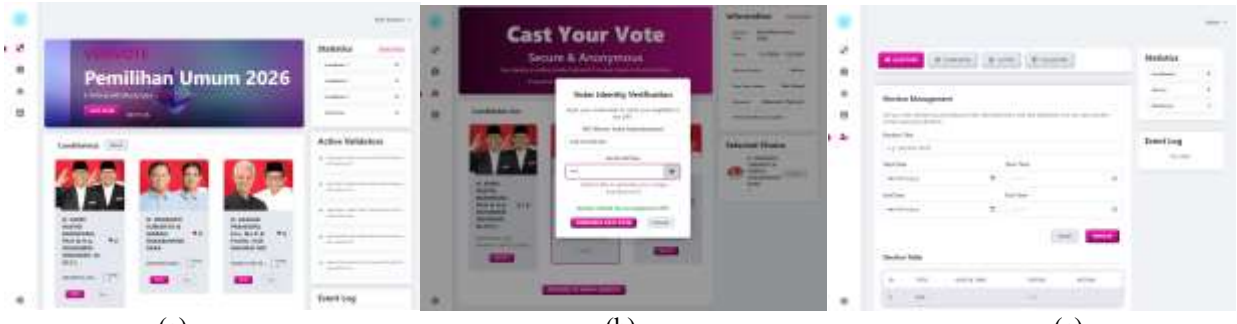
Logika inti sistem diimplementasikan melalui struktur *smart contract* modular menggunakan bahasa pemrograman *Solidity* versi 0.8.0 ke atas. Arsitektur logis kontrak ini dibagi menjadi tujuh modul utama, yaitu *Voting.sol* sebagai kontrak utama, *VotingCore.sol* untuk struktur data dasar dan menggunakan prinsip *inheritance*, *CandidateManager.sol* dan *ElectionManager.sol* untuk tata kelola administratif, *VoterManager.sol* untuk validasi pemilih, *VotingProcess.sol* untuk logika pemungutan suara, serta *ResultViewer.sol* untuk transparansi publik menggunakan fungsi *view*. Penggunaan pada modular dengan prinsip pewarisan ini tidak hanya meningkatkan auditabilitas kode, tetapi juga mengoptimalkan biaya *gas fee* dan mempermudah pemeliharaan sistem dalam jangka panjang. Integrasi antar modul ini memastikan bahwa setiap proses, mulai dari pendaftaran hingga kalkulasi hasil proses pemilihan, dapat berjalan secara sinkron dan aman di bawah aturan protokol.

3.2 Antarmuka Komponen *Front-End*

Komponen ini dirancang sebagai lapisan antarmuka pengguna (*user interface*) yang memfasilitasi interaksi pengguna dengan *smart contract* di jaringan *blockchain*. Pengembangan antarmuka ini menggunakan pustaka *React.js* untuk memudahkan manajemen status (*state management*) secara dinamis dan *Ethers.js* sebagai penyedia komunikasi (*provider*) menuju *blockchain*. Rancangan antarmuka dibagi secara modular berdasarkan peran dan fungsionalitas utama untuk menjamin pengalaman pengguna yang intuitif.

Struktur halaman dalam purwarupa ini dikelompokkan menjadi tiga kategori akses utama:

a. Halaman Utama dan Informasi: Meliputi *Homepage* yang menyajikan ringkasan statistik pemilu secara *real-time*, *Detailpage* untuk memaparkan profil lengkap kandidat yang terverifikasi, serta *Resultpage* yang menampilkan perolehan suara secara transparan setelah periode pemilihan berakhir. Halaman-halaman ini bersifat *read-only* yang ditarik langsung dari *ledger blockchain*.
b. Halaman Pemungutan Suara: Merupakan inti dari sistem bagi aktor pemilih. Halaman *CastVote* mengintegrasikan fungsi logika untuk menghasilkan *Merkle Proof* secara lokal sebelum dikirimkan ke *blockchain*. Selain itu, terdapat fitur verifikasi mandiri (*Verify My Vote*) yang memungkinkan pemilih melakukan audit mandiri terhadap status suaranya secara transparan.
c. Halaman Administrasi: *Adminpage* dengan panel kendali khusus yang hanya dapat diakses oleh otoritas (admin) dan *validator* melalui verifikasi alamat *wallet MetaMask*. Panel ini dibagi menjadi empat *tab* manajerial: *Election Management* (jadwal pemilu), *Candidate Management* (pengelolaan data kandidat), *Voter Management* (mengunggah *Merkle Root* DPT dan integrasi IPFS), serta *Validator Management* (pengelolaan akun *validator*).



(a) (b) (c)

Gambar 3. Halaman (a) Utama, (b) Pemungutan Suara, (c) dan Administrasi

Seluruh halaman pada Gambar 3, yang menerapkan pengamanan *Access Control* pada sisi klien, yang tombol aksi atau navigasi tertentu hanya akan muncul berdasarkan status identitas pengguna yang terdeteksi dari *wallet* yang terhubung. Misalnya tombol *vote* hanya akan muncul pada saat status periode pemilu sedang berlangsung atau sedang aktif dan status pengguna adalah pemilih terdaftar yang belum pernah melakukan *voting*, lalu halaman administrasi hanya dapat diakses dengan status akun yang terdeteksi sebagai otoritas (admin) atau *validator*. Hal ini memastikan bahwa integritas prosedur pemilihan tetap terjaga bahkan sebelum transaksi mencapai lapisan *blockchain*.

3.3 Analisis Kriptografi *Merkle Tree* dan Privasi Pemilih

Aspek keamanan dan privasi dalam purwarupa sistem ini dikelola melalui implementasi struktur data *Merkle Tree* untuk menjamin bahwa identitas sensitif pemilih tidak pernah tersimpan secara mentah (*plaintext*) di dalam

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1903- 1911
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/ 10.62712/juktisi.v4i3.782

blockchain. Proses ini diawali dengan transformasi data DPT (Daftar Pemilih Tetap) secara *off-chain*, di mana Nomor Induk Kependudukan (NIK) dikonversi menjadi *voter hash ID* menggunakan algoritma *hashing* SHA-256 yang dipadukan dengan kunci *salt* unik.

```
// mapping
mapping(uint256 => bytes32) public voterMerkleRoots;
// validation in func
bytes32 leaf = keccak256(abi.encodePacked(_vId, msg.sender));
require(MerkleProof.verify(_proof, voterMerkleRoots[electionId], leaf), "Invalid Proof");
```

Gambar 4. Visualisasi struktur data *Merkle Tree* dan Validasi fungsi *Merkle Proof*

Penggunaan *Merkle Tree* dalam penelitian ini memberikan solusi atas tantangan skalabilitas dan efisiensi penyimpanan pada jaringan *blockchain*. Gambar 3 menunjukkan bahwa otoritas (admin) hanya perlu mengunggah satu nilai *Merkle Root* (*32-bytes*) ke dalam *smart contract* dengan satu transaksi saja untuk mewakili keseluruhan ribuan bahkan lebih data pemilih. Ketika pemilih memberikan suara, dari sisi *front-end* akan menghitung *Merkle Proof* secara lokal berdasarkan *input* pengguna. Bukti kriptografi ini akan dikirimkan ke *smart contract* untuk divalidasi menggunakan fungsi *MerkleProof*.verify dari pustaka OpenZeppelin.
Mekanisme ini memastikan tercapainya dua parameter non-fungsional utama:

a. Pseudonimitas Identitas: *Blockchain* hanya mencatat status *hasVoted* pada alamat *wallet* yang anonim tanpa perlu mengetahui NIK asli pemilih, sehingga kerahasiaan identitas tetap terjaga (NF3.2).
b. Integritas Data *Off-Chain*: Seluruh *metadata* pemilih disimpan di jaringan IPFS dengan referensi CID yang berfungsi sebagai segel digital. Apabila terjadi perubahan sekecil apapun pada *file* DPT di IPFS, nilai CID akan berubah total, sehingga manipulasi data *off-chain* dapat dideteksi secara instan.

Melalui perpaduan penyimpanan *on-chain* untuk *root* dan penyimpanan *off-chain* untuk data terenkripsi, sistem berhasil menyeimbangkan antara transparansi audit publik dengan perlindungan privasi individu.

3.4 Implementasi Mekanisme Konsensus *Proof of Authority* (PoA)

Sistem ini menerapkan konsep dari mekanisme *Proof of Authority* (PoA) sebagai solusi untuk memitigasi risiko sentralisasi kekuasaan dan penyalahgunaan wewenang oleh otoritas tunggal. Berbeda dengan sistem *e-voting* tradisional yang memberikan kontrol penuh kepada administrator, kerangka kerja ini mengintegrasikan logika *Multi-signature Approval* atau skema *M-of-N Approval* pada fungsi-fungsi administratif yang bersifat krusial.

Dalam implementasinya, setiap aksi administratif sensitif tidak dapat dieksekusi langsung oleh otoritas (admin) seperti pendaftaran kandidat baru dan pengaturan periode waktu pemilihan hingga finalisasi resmi hasil akhir. Status data yang telah diatur oleh admin hanya akan berada pada tahap *pending*. Aktivasi data hanya akan terjadi setelah kuorum persetujuan dari mayoritas *validator* aktif sebanyak lebih dari 50%. *Validator* dalam sistem ini bertindak sebagai identitas digital dalam fungsi persetujuan di *smart contract*.

Mekanisme ini memastikan bahwa integritas pemilihan tetap terjaga meskipun akun admin mengalami kompromi keamanan. Secara teknis, setiap *validator* memberikan persetujuan melalui fungsi yang telah didefinisikan dalam *smart contract* yang memicu pencatatan suara dalam *ledger blockchain*. Setelah jumlah persetujuan memenuhi ambang batas (kuorum), status data secara otomatis akan menjadi *Approved* untuk kandidat atau *Active* untuk status periode pemilu. Dengan diterapkannya konsep PoA, sistem tidak hanya menawarkan desentralisasi teknis, tetapi juga desentralisasi operasional yang menjamin transparansi pada setiap tahapan pemilu digital.

3.5 Hasil Pengujian dan Evaluasi

Evaluasi terhadap purwarupa sistem dilakukan untuk memvalidasi fungsionalitas dan performa seluruh komponen secara *end-to-end*. Pengujian dibagi menjadi dua tahap utama: *White-box testing* untuk memvalidasi logika internal *smart contract* dan *black-box testing* untuk menguji alur kerja sama antarmuka pengguna.

3.5.1 Pengujian Logika *Smart Contract* (*White-box Testing*)

Pengujian dilakukan pada lingkungan jaringan *Ethereum* lokal menggunakan kerangka kerja *Hardhat*/*Ganache* dan *Remix IDE*. Fokus utama adalah memastikan bahwa aturan protokol pemilihan dijalankan secara otomatis tanpa celah keamanan. Pengujian *unit testing* otomatis pada *framework Hardhat* (menggunakan *library Chai* dan *Mocha*) menunjukkan tingkat keberhasilan eksekusi logika sebesar 100% pada Gambar 4.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1903- 1911
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/ 10.62712/juktisi.v4i3.782

```
>yarn workspace contracts hardhat test test/Voting.js

Voting Smart Contract (FULL COVERAGE)
  ✓ Admin & initial validator set correctly (106ms)
  ✓ Admin can add & remove validator
  ✓ Non-admin cannot manage validators (50ms)
  ✓ Create election & check status flow
  ✓ Reject invalid election time
  ✓ Add, edit & approve candidate with validators
  ✓ Reject candidate add outside Scheduled
  ✓ Set voter Merkle root only in Scheduled
  ✓ Election requires >50% validator approval to start
  ✓ Valid voter can vote once using Merkle proof
  ✓ Finalize election & save history


11 passing (630ms)
```

Gambar 5. *Unit Testing* pada *Framework Hardhat*

Tabel 1. Ringkasan Hasil Eksekusi Uji Coba Skenario Fungsi Inti *Smart Contract*

ID	Nama Fungsi	Hasil Harapan	Relasi Kebutuhan	Status
SC-01	*Modifiers*: *onlyAdmin*	Penolakan akses fungsi administratif oleh akun non-admin	NF1.3 (Kontrol Akses)	Lulus
SC-04	*setVoterMerkleRoot*	Penyimpanan *Merkle Root* (*32-bytes*) dan CID IPFS berhasil	F1.2 & NF2.3	Lulus
SC-06	*_processApproval*	Data aktif setelah mencapai kuorum *validator* (>50%)	F3.1 (*Multi-sign*)	Lulus
SC-07	*vote* (*verify*)	Verifikasi kriptografi *Merkle Proof* untuk hak suara sah	F2.1 & F2.2	Lulus
SC-08	Status: *hasVoted*	Penolakan otomatis terhadap upaya pemilihan ganda	F2.3 (*one person one vote*)	Lulus

Berdasarkan hasil pengujian pada Tabel 1, sistem terbukti mampu menegakkan prinsip *one person one vote* secara kaku melalui status *hasVoted* (SC-08). Percobaan pemilihan ganda juga dapat dicegah dengan mengonfirmasi bahwa status pemilih telah dikunci secara permanen di dalam *ledger blockchain* segera setelah transaksi pemberian suara berhasil (F2.3). Penyimpanan data melalui fungsi *setVoterMerkleRoot* (SC-04) memenuhi aspek efisiensi biaya transaksi (NF2.3). *onlyAdmin* (SC-01) yang secara konsisten melakukan penolakan akses terhadap akun non-admin atau non-otoritas menjaga kontrol akses terhadap aksi administratif (NF1.3). Dengan fungsi *_processApproval* (SC-06), aspek tata kelola berhasil mendistribusikan kewenangan administratif kepada *validator* melalui skema *multi-signature* (F3.1) dengan kuorum mayoritas sederhana. Fungsi *vote* (SC-07) mengonfirmasi akurasi verifikasi kriptografi berbasis *Merkle Proof*, yang memungkinkan sistem memvalidasi hak pilih secara sah tanpa memperlihatkan data sensitif pemilih seperti NIK di jaringan publik (F2.1 & F2.2). Secara keseluruhan, seluruh fungsi inti telah memenuhi kriteria keberhasilan dengan status lulus pada setiap skenario pengujian.

3.5.2 Pengujian Integrasi dan Antarmuka (*Black-box Testing*)

Tahap ini menguji bagaimana pengguna berinteraksi dengan sistem melalui dompet digital *MetaMask*. Pengujian mencakup sinkronisasi data *real-time* dan responsivitas antarmuka terhadap perubahan status pada *blockchain*.

(a) (b) (c)

Gambar 6. Antarmuka (a) otorisasi *digital signature MetaMask*, (b) fitur *Verify My Vote* (c), dan fitur *Recent Activity Log*

Hasil observasi menunjukkan bahwa integrasi antara *Ethers.js* dan *React Context API* yang ditunjukkan pada Gambar 6 berhasil menyajikan data secara akurat. Sebagai contoh, perolehan suara pada halaman utama diperbaharui secara otomatis segera setelah transaksi *vote* mendapatkan konfirmasi blok. Selain itu, fitur verifikasi hak suara pemilih (*Verify My Vote*) terbukti efektif memberikan transparansi mandiri. Fitur verifikasi ini mencocokkan masukan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1903- 1911
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/ 10.62712/juktisi.v4i3.782

lokal pemilih dengan *events VoteCast* yang di-*emit* oleh transaksi pemungutan suara dalam *smart contract* guna membuktikan integritas data secara *immutable*. Aspek transparansi diperkuat dengan fitur *Recent Activity Log* yang menyajikan riwayat transaksi secara dinamis dan kronologis, memastikan setiap aksi administratif maupun voting dapat diaudit langsung oleh pengguna.

3.5.3 Analisis Performa

Dari aspek kinerja, penggunaan jaringan lokal memberikan hasil yang stabil. Waktu pembuatan blok (*block time*) rata-rata tercatat di bawah 10 detik, dengan waktu respon transaksi suara antara 3 hingga 5 detik. Performa ini memenuhi kebutuhan non-fungsional (NF2.1) untuk menangani volume transaksi tinggi selama periode pemilu berlangsung tanpa mengalami kegagalan sinkronisasi pada *ledger*.

3.6 Analisis Hasil dan Pembahasan

Berdasarkan hasil implementasi dan pengujian yang telah dipaparkan, sistem *e-voting* ini terbukti mampu menjawab tantangan krusial dalam pemilihan umum digital melalui tiga pilar utama: integritas data, privasi pemilih, dan desentralisasi wewenang.

3.6.1 Integritas dan Transparansi Melalui *Immutability*

Penggunaan teknologi *blockchain* memberikan jaminan bahwa setiap suara yang masuk bersifat *immutable* atau tidak dapat diubah kembali. Tidak seperti basis data tersentralisasi yang rentan terhadap manipulasi oleh kekuasaan terpusat (*single point of control*), sistem ini mencatat setiap transaksi secara permanen. Transparansi perhitungan suara yang berjalan otomatis melalui *smart contract* (NF4.1) memastikan bahwa hasil akhir adalah akumulasi jujur dari seluruh transaksi sah di dalam *ledger*, tanpa adanya celah untuk intervensi manual yang dapat memicu kesalahan manusia (*human error*).

3.6.2 Efisiensi Verifikasi dan Perlindungan Privasi

Implementasi *Merkle Tree* terbukti menjadi solusi efektif dalam menjaga privasi data sensitif (NF3.2). Dengan memisahkan penyimpanan data pemilih secara *off-chain* dan hanya menyimpan *Merkle Root* secara *on-chain*, sistem berhasil menjaga kerahasiaan identitas pemilih namun tetap mempertahankan validasi yang absolut. Penggunaan referensi CID dari IPFS memberikan lapisan keamanan tambahan terhadap integritas data pemilih tetap. Hasil analisis menunjukkan bahwa mekanisme ini tidak hanya aman secara kriptografi, tetapi juga sangat efisien dalam penggunaan sumber daya komputasi (*gas fee*), karena beban penyimpanan pada rantai blok dikurangi secara signifikan (NF2.3).

3.6.3 Akuntabilitas Melalui Konsensus PoA

Penerapan konsep konsensus *Proof of Authority* (PoA) melalui skema *multi-signature* memberikan transformasi besar pada tata kelola pemilu digital. Dengan mewajibkan persetujuan mayoritas *validator* (>50%) untuk setiap aksi administratif, risiko penyalahgunaan wewenang (*abuse of power*) oleh otoritas tunggal berhasil dieliminasi (F3.1). Stabilitas jaringan yang ditunjukkan dengan *block time* di bawah 10 detik membuktikan bahwa kerangka kerja ini sangat layak untuk diimplementasikan pada skala pemilihan yang membutuhkan konfirmasi transaksi cepat dan latensi rendah.

Secara keseluruhan, *Hybrid Voting Framework* yang dikembangkan dalam penelitian ini berhasil menyatukan aspek transparansi publik dengan perlindungan keamanan privasi individu. Purwarupa ini telah memenuhi seluruh kriteria keberhasilan yang ditetapkan dan menawarkan standar baru bagi infrastruktur pemilu yang lebih aman, transparan, dan akuntabel.

4. KESIMPULAN

Penelitian ini telah berhasil menjawab tantangan utama dalam sistem pemilihan umum *online* (*e-voting*) melalui pengembangan *Hybrid Voting Framework* berbasis teknologi *blockchain*. Berdasarkan hasil implementasi dan pengujian, dapat disimpulkan bahwa integrasi struktur data *Merkle Tree* mampu memberikan solusi yang sangat efisien terhadap kendala skalabilitas dan biaya penyimpanan data pada rantai blok. Dengan hanya menyimpan satu nilai *Merkle Root* (*32-bytes*) untuk mewakili ribuan atau lebih data pemilih, sistem tidak hanya meminimalkan penggunaan memori pada *ledger*, tetapi juga berhasil menjaga privasi dan anonimitas identitas pemilih secara absolut tanpa mengurangi validitas hak pilihnya. Selain itu, penerapan konsep mekanisme konsensus *Proof of Authority* (PoA) melalui skema *multi-signature approval* terbukti efektif dalam memitigasi risiko penyalahgunaan wewenang oleh otoritas tunggal. Penggunaan kuorum *validator* yang mewajibkan persetujuan (>50%) untuk setiap aksi administratif krusial memberikan lapisan akuntabilitas baru yang tidak ditemukan pada sistem *e-voting* konvensional tersentralisasi. Seluruh rangkaian pengujian *white-box* dan *black-box* mengonfirmasi bahwa purwarupa ini memiliki stabilitas performa dengan waktu pembuatan blok di bawah 10 detik, serta mampu menegakkan prinsip *one person one vote* secara kaku. Transparansi yang ditawarkan melalui fitur audit mandiri, visualisasi jejak audit melalui *recent activity*

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1903- 1911
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/ 10.62712/juktisi.v4i3.782

log yang bersumber dari *events on-chain*, dan keterbukaan data pada *ledger* publik secara *real-time* berpotensi besar untuk meningkatkan kepercayaan masyarakat (*public trust*) terhadap integrasi hasil pemilu. Secara keseluruhan, model teknologi yang diusulkan dalam penelitian ini membuktikan bahwa perpaduan antara keamanan kriptografi *on-chain* dan efisiensi penyimpanan *off-chain* pada IPFS dapat menjadi standar infrastruktur baru untuk mewujudkan ekosistem demokrasi digital yang aman, transparan, dan akuntabel.

REFERENCES

[1] A. Perdana *dkk.*, *TATA KELOLA PEMILU DI INDONESIA*. Jakarta: KOMISI PEMILIHAN UMUM REPUBLIK INDONESIA, 2019.

[2] C. H. Roh dan I. Y. Lee, "A Study on Electronic Voting System Using Private Blockchain," *Journal of Information Processing Systems*, vol. 16, no. 2, hlm. 421–434, Apr 2020, doi: 10.3745/JIPS.03.0135.

[3] S. S. Sarmah, "Understanding Blockchain Technology," vol. 8, no. 2, hlm. 23–29, 2018, doi: http://dx.doi.org/10.5923/j.computer.20180802.02.

[4] A. S. Gaikwad, "Overview of Blockchain," *Int J Res Appl Sci Eng Technol*, vol. 8, no. 6, hlm. 2268–2270, Jun 2020, doi: 10.22214/ijraset.2020.6364.

[5] K. R. Ballamudi, "Blockchain as a Type of Distributed Ledger Technology," *Asian Journal of Humanity, Art and Literature*, vol. 3, no. 2, hlm. 127–136, Des 2016, doi: 10.18034/ajhal.v3i2.528.

[6] Z. Zheng, S. Xie, H. N. Dai, X. Chen, dan H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, hlm. 352, 2018, doi: 10.1504/IJWGS.2018.095647.

[7] M. Krichen, M. Ammi, A. Mihoub, dan M. Almutiq, "Blockchain for Modern Applications: A Survey," *Sensors*, vol. 22, no. 14, hlm. 5274, Jul 2022, doi: 10.3390/s22145274.

[8] C. Denis González, D. Frias Mena, A. Massó Muñoz, O. Rojas, dan G. Sosa-Gómez, "Electronic Voting System Using an Enterprise Blockchain," *Applied Sciences*, vol. 12, no. 2, hlm. 531, Jan 2022, doi: 10.3390/app12020531.

[9] J. Rosa-Bilbao dan J. Boubeta-Puig, "Ethereum blockchain platform," dalam *Distributed Computing to Blockchain*, Elsevier, 2023, hlm. 267–282. doi: 10.1016/B978-0-323-96146-2.00006-1.

[10] M. Sallal, R. de Fréin, dan A. Malik, "PVPBC: Privacy and Verifiability Preserving E-Voting Based on Permissioned Blockchain," *Future Internet*, vol. 15, no. 4, hlm. 121, Mar 2023, doi: 10.3390/fi15040121.

[11] H. Kim, K. E. Kim, S. Park, dan J. Sohn, "E-voting System Using Homomorphic Encryption and Blockchain Technology to Encrypt Voter Data," Nov 2021.

[12] U. Majeed, S. S. Hassan, Z. Han, dan C. S. Hong, "DAO-FL: Enabling Decentralized Input and Output Verification in Federated Learning with Decentralized Autonomous Organizations," 30 Mei 2024. doi: 10.36227/techrxiv.24546502.v2.

[13] P. Dhiman, S. Kumar Henge, S. Singh, A. Kaur, P. Singh, dan M. Hadabou, "Blockchain Merkle-Tree Ethereum Approach in Enterprise Multitenant Cloud Environment," *Computers, Materials & Continua*, vol. 74, no. 2, hlm. 3297–3313, 2023, doi: 10.32604/cmc.2023.030558.

[14] N. Sangeeta dan S. Y. Nam, "Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability," *Electronics (Basel)*, vol. 12, no. 7, hlm. 1545, Mar 2023, doi: 10.3390/electronics12071545.

[15] S. A. Sultana, C. Rupa, R. P. Malleswari, dan T. R. Gadekallu, "IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field," *Information*, vol. 14, no. 8, hlm. 446, Agu 2023, doi: 10.3390/info14080446.