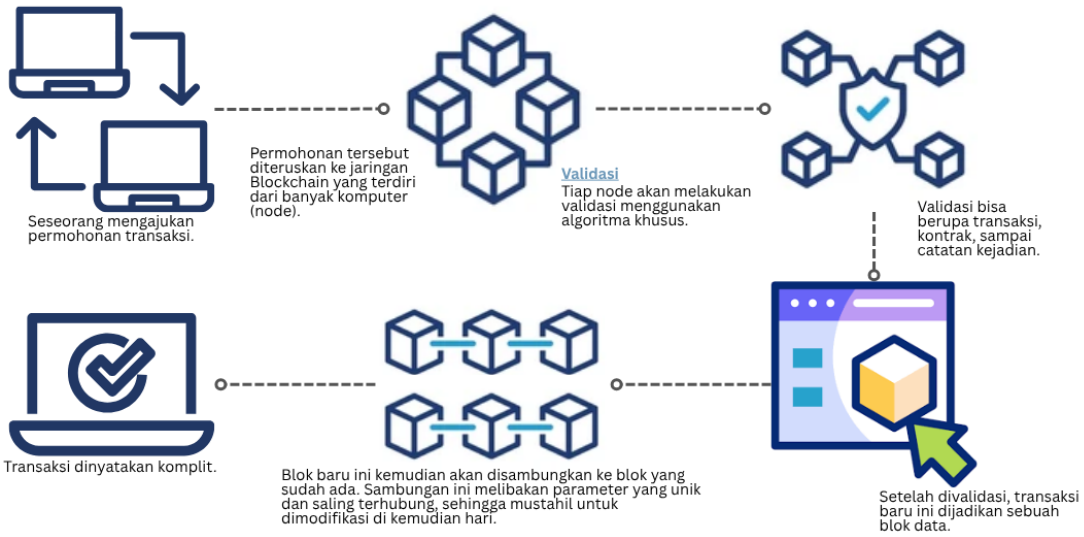
BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

2.1.1 *Blockchain* dan Implementasinya dalam *e-voting*

Blockchain merupakan teknologi pencatatan terdistribusi (*distributed ledger technology*) yang bekerja dengan menyimpan data dalam bentuk blok yang saling terhubung dan diamankan menggunakan kriptografi (Alhat & Kakade, 2024). Setiap blok berisi sekumpulan transaksi yang telah divalidasi oleh jaringan dan ditautkan secara berurutan sehingga membentuk rantai (*chain*). Struktur tersebut menjadikan *Blockchain* bersifat *immutable*, yaitu data yang sudah tercatat tidak dapat diubah atau dihapus tanpa persetujuan jaringan (Kizza, 2024). Alur kerja *Blockchain* secara umum dapat dilihat pada Gambar 2.1.



Gambar 2. 1 Alur Kerja *Blockchain*

Alur kerja *Blockchain* secara umum seperti pada Gambar 2.1 dijelaskan sebagai berikut:

a. Pengajuan Transaksi

Pengguna menginisiasi transaksi, misalnya mengirimkan informasi, melakukan transfer aset digital, atau memberikan *vote* dalam *e-voting*. Transaksi tersebut kemudian dikirimkan ke jaringan *Blockchain*.

b. Penyiaran Transaksi ke *Node* Jaringan

Transaksi yang diajukan akan disiarkan (*broadcast*) ke seluruh komputer peserta dalam jaringan yang disebut *node*. *Node* menyimpan salinan *ledger* sehingga tidak ada titik pusat kegagalan (*single point of failure*).

c. Validasi Transaksi melalui Konsensus

Setiap *node* melakukan proses validasi untuk memastikan bahwa transaksi sah dan sesuai aturan protokol. Validasi ini dilakukan melalui algoritma konsensus, misalnya, *Proof of Stake* (PoS). Proses ini memastikan seluruh *node* mencapai kesepakatan mengenai kebenaran data tanpa otoritas terpusat.

d. Pembentukan Blok (*Block Creation*)

Transaksi yang telah valid akan dikelompokkan dan disusun menjadi satu blok. Pada tahap ini, sistem menghitung *hash* kriptografis yang mengikat blok dengan blok sebelumnya untuk menjaga integritas struktur *Blockchain*.

e. Penambahan Blok ke dalam Rantai

Setelah diverifikasi, blok baru ditambahkan ke rantai blok yang sudah ada dan disiarkan kepada seluruh *node*. Setiap perubahan dapat terdeteksi karena *hash* akan menjadi tidak sesuai apabila terjadi modifikasi paksa.

f. Pencatatan Permanen dan Distribusi

Blok yang telah ditambahkan bersifat permanen, transparan, dan dapat diaudit oleh seluruh *node* dalam jaringan. Hal ini menjamin keamanan dan kepercayaan terhadap data yang tersimpan.

Blockchain merupakan teknologi pencatatan transaksi yang bersifat desentralisasi, transparan, dan tidak dapat diubah, sehingga menjadikannya solusi yang potensial untuk diterapkan dalam sistem *e-voting* (Revanth dkk., 2024). Implementasi *Blockchain* dalam *e-voting* juga dapat mengoptimalkan efisiensi proses pemungutan dan penghitungan hasil *voting*, karena seluruh data tersimpan secara terdesentralisasi dalam jaringan yang aman dan terenkripsi (Syaifudin dkk., 2024).

Blockchain memfasilitasi transparansi, keamanan, dan efisiensi dalam proses pemungutan hasil *voting*, meskipun metode yang digunakan dapat bervariasi tergantung pada persyaratan spesifik (Khaldun, 2025). *Public Blockchain* menawarkan transparansi yang lebih tinggi dengan memungkinkan siapa saja untuk memverifikasi transaksi secara terbuka, sementara *Private Blockchain* memprioritaskan efisiensi dan kontrol yang lebih ketat dalam lingkungan yang tertutup (Sedlmeir dkk., 2022).

Konteks *e-voting* memanfaatkan cara kerja *Blockchain* yang memungkinkan pencatatan hasil *voting* secara transparan karena seluruh transaksi dapat dilihat dan diverifikasi oleh publik. Keamanan data terjamin melalui mekanisme hash serta struktur blok yang mencegah modifikasi terhadap hasil *voting* setelah dicatat di *Blockchain*. Proses ini tidak memerlukan perantara, sebab *Smart Contract* secara otomatis menangani seluruh prosedur penghitungan hasil *voting*.

2.1.2 *Smart Contract* dalam *e-voting*

Smart Contract adalah program komputer yang dieksekusi secara otomatis pada *Blockchain* berdasarkan aturan yang telah ditetapkan dalam kode (Lin dkk., 2025). Dalam konteks *e-voting*, *Smart Contract* berfungsi sebagai "aturan pemilihan digital" yang bersifat *immutable* dan transparan (Wahyudi dkk., 2025).

Smart Contract dalam sistem *e-voting* berfungsi sebagai penegak aturan, mesin status (*state machine*), sumber kebenaran, *audit trail*, dan mekanisme transparansi sekaligus. Penegak aturan pada *contract* memastikan hanya *wallet* terverifikasi yang dapat memberikan *vote* melalui pemeriksaan seperti `require(voters[msg.sender].isVerified, "Not verified")`, serta mencegah *double voting* dengan pengecekan dan pembaruan *flag* `hasVoted` secara atomik. Fungsi *voting* juga dibatasi agar hanya dapat dipanggil saat periode pemilihan aktif, sementara fungsi sensitif hanya dapat dijalankan oleh alamat admin yang berwenang. Peran *contract* sebagai *state machine* terlihat pada pengaturan transisi status pemilihan dari *Created* → *Started* →

Ongoing → *Ended* → *Finalized*, di mana setiap perpindahan status mensyaratkan kondisi khusus dan hanya dapat dieksekusi sekali untuk menjaga konsistensi proses.

Smart Contract berfungsi sebagai *single source of truth*, yaitu daftar kandidat resmi, hasil *voting* yang sah, status verifikasi pemilih, dan konfigurasi pemilihan tersimpan di dalamnya serta tidak dapat diubah setelah dicatat. Semua interaksi terekam permanen di *ledger* sehingga membentuk *audit trail*, setiap *voting* memiliki *transaction hash* unik, cap waktu, alamat pelaku, dan parameter yang digunakan, yang memungkinkan siapa pun memverifikasi kejadian melalui *block explorer*. Dukungan terhadap transparansi publik diberikan melalui fungsi *view* seperti `getResults()`, `getCandidates()`, dan `getVoterStatus(address)` yang dapat dipanggil tanpa *gas fee*, sehingga verifikasi publik dapat dilakukan tanpa beban biaya.

Keunggulan penggunaan *Smart Contract* untuk *e-voting* meliputi otomasi (penghitungan hasil *voting* tanpa operator manual), *immutability* (hasil tidak dapat dimodifikasi setelah tercatat), transparansi (kode dapat diaudit publik), *trustlessness* (mengurangi kebutuhan mempercayai pihak ketiga), *verifiability* (setiap pemilih dapat memeriksa bahwa *vote*-nya tercatat), dan efisiensi biaya (mengurangi beban operasional penyelenggaraan) (Wahyudi dkk., 2025).

Arsitektur sistem menempatkan *Smart Contract* sebagai komponen sentral, antarmuka pengguna (UI) berkomunikasi dengan Web3 *provider* seperti *MetaMask* melalui Web3/Ethers.js, yang kemudian memanggil *core logic* pada `Election.sol`. Eksekusi dan penyimpanan ditangani oleh jaringan

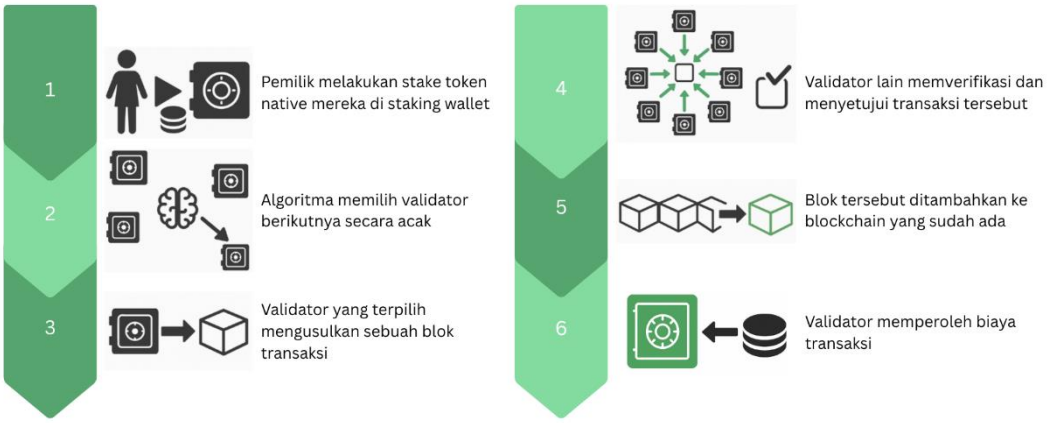
Blockchain (*Polygon*) yang dipelihara validator PoS, dengan hasil akhir tercatat pada *distributed ledger*. Secara ringkas, alur *end-to-end* mencakup:
User Interface → Web3 *Provider* (*MetaMask*) → *Smart Contract* (`Election.sol`) [*CORE LOGIC*] → *Blockchain Network* (*Polygon*) → *Validator Nodes* (PoS *Consensus*) → *Distributed ledger*.

2.1.3 Algoritma Konsensus PoS (*Proof of Stake*)

Algoritma konsensus merupakan mekanisme fundamental dalam sistem *Blockchain* yang memastikan semua *node* dalam jaringan mencapai kesepakatan mengenai keabsahan transaksi tanpa memerlukan otoritas terpusat (Li & Kang, 2024). *Proof of Stake* (PoS) adalah salah satu mekanisme konsensus *Blockchain* yang berbeda secara fundamental dari *Proof of Work* (PoW).

Proof of Stake memilih validator untuk membuat blok baru berdasarkan jumlah token yang mereka pertaruhkan (*stake*) dalam jaringan, bukan melalui kompetisi komputasi intensif sebagaimana terjadi pada PoW (Haodic, 2025). Konsep "*stake*" merujuk pada sejumlah *cryptocurrency* yang dikunci oleh validator sebagai jaminan kejujuran mereka. Semakin besar jumlah token yang dipertaruhkan, semakin tinggi probabilitas validator tersebut dipilih untuk mengusulkan blok berikutnya (Salau dkk., 2022).

Mekanisme konsensus PoS ini secara keseluruhan dapat dilihat pada Gambar 2.2.



Gambar 2. 2 Mekanisme Konsensus PoS

Gambar 2.2 menggambarkan Mekanisme PoS bekerja melalui serangkaian tahapan yang saling terkait:

a. *Staking* dan Registrasi Validator

Calon validator harus mengunci sejumlah minimum token sebagai *stake*, termasuk pada ekosistem *Polygon* yang mewajibkan *staking* token POL melalui *Smart Contract* khusus. Mekanisme ini menciptakan insentif ekonomi agar validator tetap jujur, karena *stake* dapat disita (*slashing*) ketika terjadi pelanggaran (Bhudia dkk., 2023).

b. Pemilihan Validator (*Validator Selection*)

Algoritma PoS menggunakan mekanisme *pseudorandom* untuk menentukan validator yang berhak mengusulkan blok berikutnya. Pemilihan dipengaruhi oleh jumlah *stake weight*, *age of stake*, serta elemen randomisasi yang mencegah munculnya pola pemilihan yang mudah ditebak (Gurram dkk., 2023).

c. Proposal dan Validasi Blok

Validator terpilih bertugas mengumpulkan transaksi dari *mempool*, memverifikasi keabsahannya, lalu menyusunnya menjadi blok baru. Setelah blok terbentuk, validator tersebut mengusulkannya kepada validator lain untuk diperiksa dan diproses dalam konsensus (Heimbach dkk., 2023).

d. Atestasi dan Konsensus

Validator lain memberikan atestasi dengan memverifikasi secara independen seluruh transaksi dalam blok dan menandatanganinya secara kriptografis. Blok dinyatakan sah dan dapat ditambahkan ke *Blockchain* setelah memperoleh persetujuan dari minimal dua pertiga validator aktif (Leonardos, 2018).

e. Finalisasi dan Penambahan Blok

Setelah mencapai *threshold* konsensus, blok baru ditambahkan ke *Blockchain*. Sistem *Polygon* menggunakan mekanisme *checkpoint* tambahan untuk memastikan *finality* dengan mengirimkan *snapshot state* ke *Ethereum mainnet* setiap 256 blok (Paul, 2023).

Mekanisme keamanan ekonomi dalam PoS diterapkan melalui berbagai sistem yang dirancang untuk menjaga integritas jaringan. Salah satu mekanisme utamanya adalah *slashing*, yaitu penalti ekonomi bagi validator yang melakukan pelanggaran seperti *double-signing*, tidak aktif dalam periode tertentu, atau memvalidasi transaksi yang tidak sesuai dengan aturan protokol.

Penalti ini dapat berupa pengurangan sebagian hingga seluruh *stake*, sehingga menciptakan disinsentif kuat terhadap perilaku berbahaya.

PoS modern mampu mengatasi masalah klasik *nothing-at-stake* melalui kombinasi mekanisme *slashing*, penggunaan *finality gadget* yang membuat pembalikan blok tidak rasional secara ekonomi, serta perlindungan terhadap *long-range attack* melalui *checkpointing* berkala (T. dkk., 2025). Konsep *economic finality* kemudian memastikan bahwa pembalikan transaksi yang telah difinalisasi akan membutuhkan biaya ekonomi yang sangat besar, sehingga membuat upaya serangan menjadi tidak menguntungkan bagi pihak mana pun.

Penerapan PoS dalam sistem *e-voting* memberikan sejumlah keunggulan yang relevan untuk kebutuhan pemilihan modern. Aspek efisiensi energi menunjukkan bahwa PoS mampu mengurangi konsumsi hingga sekitar 99% dibandingkan PoW, sehingga lebih ramah lingkungan dan cocok diterapkan pada sistem *voting* yang digunakan berulang (Shi dkk., 2023). PoS juga menawarkan skalabilitas tinggi dengan kemampuan memproses ribuan transaksi per detik, memungkinkan penyelenggaraan pemilihan berskala besar tanpa mengalami penurunan kinerja yang signifikan (Yang dkk., 2020). Biaya transaksi menjadi jauh lebih rendah karena tidak memerlukan proses penambangan yang intensif, menjadikan implementasi *e-voting* lebih ekonomis (John dkk., 2020).

Pengalaman pengguna turut meningkat berkat finalitas yang cepat, yang membuat hasil *voting* tercatat secara pasti hanya dalam hitungan detik sehingga

pemilih dapat memperoleh umpan balik hampir *real-time* (Pasupuleti, 2025). Keunggulan lain terlihat pada aspek keamanan ekonomi, karena mekanisme penetapan minimum *stake* memungkinkan biaya serangan terhadap jaringan dirancang agar tidak rasional secara finansial (Deb dkk., 2024).

PoS berperan sebagai lapisan konsensus (*Consensus layer*) dalam arsitektur *Blockchain* dan bekerja secara terpadu dengan beberapa komponen penting lainnya. *Execution layer* menjalankan *Smart Contract* yang mengatur logika aplikasi, sementara *Network layer* bertugas mengoordinasikan propagasi transaksi dan blok antar-*node*. Lapisan konsensus, dalam konteks ini PoS, berperan memastikan tercapainya kesepakatan mengenai *state Blockchain*, sementara *data layer* bertugas menyimpan *state* beserta riwayat transaksi (Hossain dkk., 2024).

2.1.4 Proses Detail Validasi dalam Sistem *e-voting*

Validator mempunyai peran krusial dalam menjaga keamanan, integritas, dan konsistensi sistem *e-voting* berbasis *Blockchain*. Jaringan *Polygon* yang menggunakan PoS mengandalkan validator untuk memvalidasi setiap transaksi yang memanggil fungsi *Smart Contract*, mengusulkan blok baru, mengumpulkan atestasi dari validator lain, serta menambahkan blok yang telah terfinalisasi ke rantai sehingga *state contract* terbarui secara kolektif (Leonardos, 2018).

Penjelasan mengenai posisi validator dalam alur sistem *e-voting* adalah sebagai berikut. Pemilih mengirim transaksi *voting* yang telah ditandatangani melalui *MetaMask,* lalu transaksi tersebut masuk ke *mempool* dan menunggu

validasi. Validator mengeksekusi verifikasi *signature* serta aturan bisnis yang terdapat di *Smart Contract*. Validator terpilih kemudian mengusulkan blok yang memuat transaksi-transaksi valid. Validator lain memberikan atestasi terhadap blok tersebut. Setelah mencapai *supermajority*, blok ditambahkan ke *chain* dan *state Smart Contract* diperbarui. Proses ini memastikan bahwa setiap perubahan *state* seperti pencatatan hasil *voting* atau perubahan status pemilih hanya terjadi setelah melewati mekanisme konsensus PoS, sehingga aspek teknis *Smart Contract* terikat dengan jaminan integritas dari *layer* konsensus.

Proses validasi dalam sistem *e-voting* berbasis *Polygon* PoS berlangsung melalui beberapa tahap yang sepenuhnya otomatis tanpa intervensi manual. Tahap awal proses konsensus mewajibkan validator melakukan *staking* token POL sebagai jaminan keikutsertaan. Jumlah token yang dikunci menentukan probabilitas mereka terpilih sebagai proposer blok, dan seluruh mekanisme registrasi serta pemilihan validator berlangsung otomatis melalui protokol. Ketika pemilih mengirim *vote*, transaksi masuk ke *mempool* dan melewati proses validasi otomatis berupa verifikasi *digital signature*, pengecekan *double voting* melalui *state Smart Contract*, verifikasi kecukupan *gas fee*, serta pemeriksaan kelayakan pemilih seperti status verifikasi dan periode *voting*. Begitu transaksi dinyatakan valid, sistem memilih *validator proposer* secara *pseudorandom* berdasarkan *stake* dan faktor randomisasi. Validator yang terpilih inilah yang mengumpulkan transaksi valid dari *mempool*, menyusunnya ke dalam blok baru, lalu menyiarkan blok tersebut ke seluruh jaringan.

Validator lain kemudian melakukan *attestation* dengan memverifikasi ulang seluruh transaksi dalam blok, mengeksekusi kembali *state transition*, dan memastikan blok mematuhi aturan protokol. Validitas blok mendorong para validator untuk memberikan *signature* sebagai bentuk persetujuan, dan konsensus tercapai ketika lebih dari dua pertiga validator memberikan *attestation*. Konsensus yang telah terbentuk membuat blok dapat ditambahkan ke rantai utama, sehingga *state Blockchain* diperbarui secara otomatis. *Polygon* kemudian mengirim *checkpoint* ke *Ethereum* setiap 256 blok guna memberikan finalitas tambahan. *Proposer* dan validator yang berkontribusi dalam proses atestasi menerima *reward* secara otomatis melalui *Smart Contract* yang menangani distribusinya (Heimbach dkk., 2023).

Proses dalam sistem *e-voting* berbasis *Blockchain* sebagian besar berlangsung secara otomatis tanpa intervensi manusia. Mekanisme seperti pemilihan *validator proposer*, validasi *signature* dan transaksi, pengecekan *double voting*, verifikasi *gas fee*, proses *attestation* dan pencapaian konsensus, finalisasi blok, distribusi *reward*, mekanisme *slashing*, hingga pengiriman *checkpoint* ke *Ethereum* sepenuhnya dijalankan oleh protokol secara deterministik. Satu-satunya bagian yang melibatkan intervensi manusia adalah proses verifikasi identitas pemilih pada *layer* aplikasi yang dilakukan oleh admin. Begitu identitas diverifikasi, seluruh proses berikutnya, mulai dari validasi transaksi *voting* di *Blockchain* hingga pencatatan dan penghitungan hasil *voting*, berjalan sepenuhnya otomatis dan tidak bergantung pada manusia, sehingga meningkatkan keamanan, akurasi, serta integritas sistem *e-voting*.

Distribusi validator dalam jaringan *Polygon* menunjukkan tingkat desentralisasi yang tinggi. Lebih dari seratus validator aktif yang tersebar di berbagai negara dan zona waktu, jaringan ini tidak memiliki *single point of failure* dan tetap beroperasi meskipun terjadi gangguan regional. Tidak ada validator tunggal yang mengendalikan jaringan karena keputusan konsensus memerlukan persetujuan *supermajority* (>2/3), menjadikan manipulasi tidak hanya sulit tetapi juga tidak rasional secara ekonomi. Seluruh aktivitas validator dapat diaudit secara publik melalui berbagai alat seperti *Polygonscan Validator Dashboard*, statistik produksi blok, catatan *slashing*, dan distribusi *stake*, sehingga publik dapat memverifikasi kejujuran sistem meskipun proses validasinya berlangsung otomatis.

Pada akhirnya, validator berfungsi sebagai *automated trust layer* dalam sistem *e-voting*. Mereka tidak memeriksa konten *vote* secara manual, tetapi menjalankan algoritma deterministik yang sama untuk mencapai konsensus melalui mekanisme kriptografis. Keamanan terjaga melalui insentif dan penalti ekonomi yang otomatis, tanpa ruang untuk bias atau preferensi pribadi. Berkat desentralisasi, tidak ada entitas tunggal yang mampu memanipulasi hasil. Peran validator menyediakan infrastruktur yang otomatis, *trustless*, dan terdesentralisasi, sehingga setiap *vote* tercatat dengan benar, tidak dapat diubah, serta dapat diverifikasi secara publik tanpa memerlukan kepercayaan pada individu validator mana pun.

2.1.5 *Polygon*

Polygon (sebelumnya *Matic Network*) merupakan solusi *layer-2 Ethereum* yang dirancang untuk meningkatkan skalabilitas dan efisiensi transaksi *Blockchain*. *Polygon* memiliki arsitektur berlapis yang dirancang untuk meningkatkan skalabilitas tanpa mengorbankan keamanan dari *Ethereum*. Secara struktural, *Polygon* terdiri dari *Ethereum layer* yang menyediakan keamanan dan finalitas, *Heimdall layer* yang menangani validator, *staking*, dan *checkpointing*, *Bor layer* sebagai *block producer* dengan kecepatan pemrosesan tinggi, serta *Execution layer* tempat eksekusi transaksi dan *Smart Contract* berlangsung (Paul, 2023). *Polygon* menggunakan konsensus *Proof of Stake* (PoS) yang dimodifikasi, di mana *checkpoint* dikirimkan secara berkala ke *Ethereum* mainnet untuk menjamin finalitas dan keamanan tambahan (Kapengut & Mizrach, 2023). Validator dipilih melalui *on-chain staking* sesuai aturan protokol.

Keunggulan utama *Polygon* dalam konteks *e-voting* meliputi kinerja tinggi dengan *block time* sekitar 2 detik dan *throughput* hingga ribuan transaksi per detik, biaya transaksi yang sangat rendah sehingga mendukung *voting* massal yang ekonomis (Duong dkk., 2023), serta keamanan berlapis yang menggabungkan mekanisme PoS dan proteksi keamanan dari *Ethereum* (Schwarz-Schilling dkk., 2022). *Polygon* juga memiliki kompatibilitas penuh dengan ekosistem *Ethereum*, termasuk dukungan terhadap bahasa pemrograman *Solidity* serta alat pengembangan populer seperti Web3.js,

Ethers.js, dan *MetaMask*, yang memudahkan proses implementasi maupun integrasi sistem *e-voting* berbasis *Blockchain* (Desai dkk., 2023).

2.1.6 Posisi dan Integrasi Komponen dalam Arsitektur *Blockchain*

Pemahaman menyeluruh mengenai cara kerja sistem *e-voting* berbasis *Blockchain* memerlukan penelusuran terhadap interaksi setiap komponen dalam arsitektur berlapis *Blockchain. Proof of Stake* (PoS) bukanlah teknologi yang berdiri sendiri, melainkan bagian inti dari *Consensus layer* yang memastikan seluruh node mencapai kesepakatan mengenai validitas transaksi, urutan blok, dan finalitas *state* (Barinov dkk., 2021).

Arsitektur *Blockchain* seperti *Polygon* yang digunakan dalam penelitian ini memiliki pembagian fungsi yang jelas pada setiap lapisannya. *Application layer* menangani interaksi pengguna melalui DApp dan Web3. *Execution layer* menjalankan *Smart Contract* dan mengelola *state* melalui EVM. *Consensus layer* tempat PoS beroperasi memilih validator, memproses proposal blok, dan mengoordinasikan *attestation*. *Network layer* menyebarkan transaksi dan blok antar-*node*. *Data layer* menyimpan seluruh riwayat dan *state Blockchain*. Pembagian fungsi tersebut membuat PoS berperan sebagai mekanisme yang memvalidasi dan menyepakati hasil eksekusi *Smart Contract*, bukan menggantikan perannya, sekaligus memastikan integritas data melalui mekanisme ekonomi, kriptografi, serta koordinasi validator yang terdistribusi.

2.1.7 *Hybrid Model* dalam *e-voting*

Hybrid Model dalam *e-voting* merupakan pendekatan yang mengintegrasikan mekanisme validasi terpusat dengan pencatatan berbasis

Blockchain untuk menyeimbangkan efisiensi dan transparansi dalam sistem pemungutan hasil *voting* digital (Nikhare, 2024). Model ini dirancang untuk mengoptimalkan kecepatan pemrosesan hasil *voting* sekaligus memastikan keamanan dan keabsahan data yang tersimpan di *Blockchain*. Validasi terpusat memungkinkan otoritas terkait untuk mengelola dan mengautentikasi pemilih dengan lebih cepat, sementara pencatatan berbasis *Blockchain* menjamin bahwa setiap hasil *voting* yang diberikan terekam secara permanen dan tidak dapat dimanipulasi (Ahmadieh & El Madhoun, 2024).

Beberapa penelitian menganalisis dan mendukung penerapan *Hybrid Model* karena kemampuannya mengatasi berbagai tantangan yang dihadapi oleh sistem *e-voting* yang sepenuhnya terdesentralisasi maupun sistem terpusat tradisional. Model ini mengurangi risiko latensi tinggi dan konsumsi sumber daya berlebihan yang sering terjadi pada sistem *Blockchain* murni, sekaligus meminimalkan potensi penyalahgunaan wewenang yang dapat terjadi dalam sistem terpusat (Tang dkk., 2023; Wang dkk., 2023).

2.1.8 Keamanan dalam *e-voting*

Keamanan merupakan aspek krusial dalam sistem *e-voting* berbasis *Blockchain,* karena menyangkut kepercayaan publik terhadap hasil *voting* yang transparan dan akurat. Seluruh penelitian yang menganalisis sistem ini menunjukkan bahwa keamanan data dan integritas hasil *voting* harus diprioritaskan untuk menghindari potensi manipulasi, serangan siber, dan akses tidak sah (Chukwudi dkk., 2024; Maddhi dkk., 2024; Pastushenko & Krasnozheniuk, 2022). Perlindungan sistem ditingkatkan melalui penerapan

berbagai metode keamanan, seperti enkripsi data *voting* dan identitas, autentikasi ketat pemilih, serta pencatatan berbasis *Blockchain* yang mencegah perubahan atau penghapusan data setelah terekam.

2.1.9 Transparansi Data dalam *e-voting*

Transparansi merupakan aspek fundamental dalam sistem *e-voting* berbasis *Blockchain*, dan evaluasi dalam penelitian ini dilakukan melalui analisis kemampuan sistem menyediakan *audit trail* yang lengkap serta dapat diverifikasi public (Syaifudin dkk., 2024). Konteks sistem *e-voting* menempatkan transparansi data sebagai prasyarat utama untuk memastikan bahwa seluruh proses pemilihan berlangsung secara terbuka, dapat diverifikasi, dan bebas dari manipulasi.

Transparansi tidak hanya berkaitan dengan kemampuan publik untuk melihat hasil akhir, tetapi juga mencakup keterbukaan terhadap setiap langkah yang terjadi di sepanjang proses pemilihan, mulai dari pencatatan *vote*, eksekusi transaksi, hingga pembaruan *state* dalam *Blockchain* (Ali dkk., 2025). Penyediaan akses penuh terhadap data transaksi dan mekanisme kerja *Smart Contract* membuat sistem *e-voting* berbasis *Blockchain* memungkinkan siapa pun memeriksa integritas proses secara independen tanpa harus mempercayai penyelenggara, validator, ataupun pihak ketiga lainnya.

2.1.10 Perbandingan Sistem Terpusat, Desentralisasi, dan *Hybrid*

Pada sistem terpusat (*centralized*), seluruh data pemilihan disimpan dalam satu server dan dikendalikan sepenuhnya oleh admin. Keunggulan sistem ini terletak pada kecepatan tinggi karena tidak memerlukan mekanisme konsensus,

biaya operasional yang relatif rendah, serta kemudahan dalam penerapan dan pengelolaan, sehingga cocok digunakan oleh organisasi berskala kecil (González dkk., 2022). Sistem terpusat tetap memiliki kelemahan mendasar, seperti adanya *single point of failure*, potensi manipulasi data oleh admin, tingkat transparansi yang rendah, serta ketiadaan *audit trail* independen (Islam & Apu, 2024).

Berbeda dengan itu, sistem desentralisasi penuh (*fully decentralized*) mendistribusikan seluruh data ke banyak *node* tanpa adanya otoritas tunggal (Troncoso dkk., 2017). Validasi dilakukan melalui algoritma konsensus seperti *Proof of Work* (PoW) atau *Proof of Stake* (PoS), sehingga menghasilkan transparansi maksimal, ketahanan terhadap manipulasi, serta *audit trail* permanen yang dapat diverifikasi publik. Sistem ini tetap memiliki sejumlah keterbatasan, antara lain biaya transaksi yang tinggi, terutama pada jaringan *Ethereum mainnet*, kecepatan pemrosesan yang lambat akibat proses konfirmasi blok, kompleksitas teknis yang tinggi, serta tantangan dalam memverifikasi identitas pengguna di luar rantai (*off-chain*) (N. C. Singh dkk., 2025).

Pendekatan *Hybrid Model* pada penelitian ini menggabungkan keunggulan sistem terpusat dan sistem desentralisasi. Proses validasi identitas pemilih dilakukan secara terpusat oleh admin, sedangkan pencatatan serta penyimpanan hasil *voting* dijalankan secara desentralisasi melalui jaringan *Blockchain*. Model ini menghadirkan keseimbangan antara efisiensi dan keamanan melalui validasi yang cepat, hasil *voting* yang transparan serta dapat

diaudit publik, dan biaya transaksi rendah berkat pemanfaatan *Polygon layer-2*. Ketergantungan terhadap kepercayaan pada admin serta kebutuhan edukasi pengguna masih menjadi tantangan, namun *Hybrid Model* tetap terbukti sebagai solusi praktis dan skalabel untuk penerapan *e-voting* di lingkungan organisasi nyata.

Tabel 2. 1 Perbandingan Sistem Terpusat, Desentralisasi, dan *Hybrid*

Aspek	**Terpusat (*Centralized*)**	**Desentralisasi Penuh (*Fully Decentralized*)**	***Hybrid Model* (Penelitian Ini)**
Struktur	Semua data dikendalikan oleh server dan admin pusat.	Data tersebar di banyak *node* tanpa otoritas tunggal.	Validasi terpusat, pencatatan desentralisasi di *Blockchain*.
Validasi	Admin memverifikasi seluruh proses.	Melalui algoritma konsensus (PoW/PoS).	Identitas diverifikasi admin, hasil diverifikasi validator PoS.
Keamanan	Rentan manipulasi dan kegagalan tunggal.	Sangat aman dan *immutable*.	Aman, namun tetap ada elemen *trust* terhadap admin.
Transparansi	Rendah, hanya admin yang dapat mengakses data.	Tinggi, semua transaksi dapat diverifikasi publik.	Tinggi, hasil dapat diaudit publik melalui *Blockchain*.
Efisiensi & Biaya	Cepat dan murah.	Lambat dan biaya tinggi.	Cepat dan biaya rendah (*Polygon layer-2*).
Kelemahan	*Single point of failure*, tidak transparan.	*Gas fee* tinggi, sulit validasi identitas.	Masih butuh kepercayaan admin dan edukasi pengguna.
Cocok Untuk	Organisasi kecil atau internal.	Komunitas *Blockchain* murni.	Organisasi nyata dengan kebutuhan efisiensi dan transparansi.

Hasil perbandingan menunjukkan bahwa *Hybrid Model* yang diusulkan mampu menggabungkan efisiensi validasi identitas dari sistem terpusat dengan keamanan dan transparansi pencatatan berbasis *Blockchain*. Pendekatan ini membuat *e-voting* lebih layak diterapkan, terutama bagi institusi yang memerlukan keseimbangan antara kontrol terpusat dan transparansi publik.

2.2 *State of the Art*

Penelitian terdahulu telah mengeksplorasi berbagai pendekatan *e-voting* berbasis *Blockchain*. Rangkuman penelitian relevan beserta gap yang diisi oleh penelitian ini disajikan pada Tabel 2.2.

Tabel 2. 2 *State of The Art*

Penelitian	**Fokus Penelitian**	**Kelebihan**	**Keterbatasan (*Gap*)**	***Research Gap* yang Diisi Penelitian Ini**
Optimizing E-voting model based on Blockchaintechnology to enhance privacy and transparency (Galal dkk., 2024)	Model *e-voting* baru menggunakan *Blockchain* (*Hyperledger Fabric*) dan enkripsi ganda (AES & RSA) guna meningkatkan keamanan, privasi pemilih, dan transparansi *voting*.	Menjamin kerahasiaan, transparansi, dan integritas hasil *voting* dengan kinerja cepat (1,7 detik/*vote*) serta keamanan ganda (biometrik & OTP).	Masalah skalabilitas, kebutuhan internet stabil, serta belum terujinya aspek *usability* dan konteks *voting* nasional.	Penelitian ini mengisi gap skalabilitas & *usability* dengan menawarkan *Hybrid Model* berbasis *Polygon* PoS yang lebih efisien dan teruji untuk skala organisasi.
Hybrid-Blockchain-Based Electronic Voting Machine System Embedded with Deepface, Sharding, and Post-Quantum Techniques (Joni dkk., 2024)	Pengembangan sistem *e-voting Blockchain* yang aman, transparan, dan skalabel dengan integrasi teknologi mutakhir seperti HAC, *sharding*, kriptografi pasca-kuantum, MPC, dan autentikasi biometrik *DeepFace*.	Sistem *e-voting* canggih dengan keamanan, skalabilitas, dan transparansi yang teruji (181 TPS) serta memenuhi aspek legal.	Keterbatasan dalam desentralisasi, validasi data riil, dan kompleksitas teknis untuk implementasi skala besar.	Menyederhanakan kompleksitas teknis dengan *Hybrid Model* yang menggabungkan validasi terpusat dan *Blockchain* PoS, sehingga lebih praktis untuk implementasi nyata.
Blockchain-Based E-voting System: A Decentralized Approach on the Ethereum Private Network (Syaifudin dkk., 2024)	Sistem *e-voting* berbasis *Ethereum* dengan *Smart Contract* untuk verifikasi identitas dan penghitungan hasil *voting* yang diakses via aplikasi *mobile*.	Sistem *e-voting Blockchain* dengan *Smart Contract* dan aplikasi *mobile* yang aman, transparan, *user-friendly*, dan terbukti stabil meski ada *delay* sinkronisasi awal.	Masalah teknis khas *Ethereum* (skalabilitas, *immutability*) dan hambatan adopsi (edukasi *Blockchain* serta infrastruktur yang belum merata).	Mengatasi keterbatasan *Ethereum* (*Gas fee* tinggi & skalabilitas rendah) dengan memanfaatkan *Polygon layer-2* dan *Hybrid Model* untuk efisiensi.
Design and Implementation of a Secure and Transparent	Sistem *e-voting Blockchain* dengan enkripsi hibrida untuk	Meningkatkan keamanan dan transparansi, sementara	Tidak mencakup kritik, batasan, atau analisis	Melengkapi sistem enkripsi hibrida dengan *Hybrid Model*

Penelitian	Fokus Penelitian	Kelebihan	Keterbatasan (*Gap*)	*Research Gap* yang Diisi Penelitian Ini
E-voting System Using Blockchain Technology and Hybrid Encryption; the case of Africa (Jnr dkk., 2024)	Afrika yang menekankan transparansi, integritas, dan aksesibilitas melalui fitur multi-faktor dan opsi *voting online/offline*.	enkripsi hibrida menjamin anonimitas dan integritas hasil *voting*.	kelemahan dari sistem yang diusulkan.	yang menambahkan validasi terpusat dan *Smart Contract* pada *Polygon* agar lebih praktis dan transparan.
Electronic voting system using Blockchain technology (Nicolae-Marian, 2024)	Aplikasi *e-voting* berbasis *Blockchain* simulasi (C/C#) untuk anonimitas, pencegahan kecurangan, dan ketersediaan sistem.	Sistem *e-voting* anonim dan tahan gangguan dengan *Blockchain* untuk integritas transparan, dilengkapi antarmuka lengkap untuk konfigurasi, *voting*, dan eksplorasi data.	Skalabilitas, keamanan lanjutan, portabilitas, serta belum diuji untuk adopsi publik dan integrasi hukum.	Mengisi gap skalabilitas & integrasi hukum dengan rancangan *Hybrid Model* berbasis *Polygon* yang lebih siap diterapkan di organisasi.
Development of an Electronic Voting System using Blockchain Technology and Deep Hybrid Learning (Based dkk., 2024)	Sistem *e-voting* dengan autentikasi sidik jari berbasis *Hybrid deep learning* dan *Blockchain* untuk keamanan dan transparansi hasil *voting*.	Sistem *e-voting* dengan akurasi biometrik 99,32% berkat model *Hybrid* dan dataset besar, didukung *Blockchain* untuk keamanan serta aplikasi web yang mudah digunakan.	Dataset *non-multimodal*, belum diuji skala besar, *usability* terbatas, dan konsensus *Blockchain* yang belum siap untuk *voting* nasional.	Melengkapi autentikasi biometrik dengan efisiensi transaksi PoS di *Polygon*, sehingga sistem lebih ringan dan praktis.
Blockchain-Powered E-voting: A Novel Approach to Secure Voter Authentication, Online Voting and Election Automation (Sujatha dkk., 2024)	Sistem *e-voting* dengan autentikasi biometrik, *Smart Contract Ethereum*, dan penyimpanan terdesentralisasi (IPFS).	Sistem *e-voting* dengan *Smart Contract*s, autentikasi multi-faktor, penyimpanan IPFS, dan antarmuka *Django* untuk keamanan, transparansi, dan kemudahan penggunaan.	Uji skala besar, dukungan regulasi, analisis teknis *Ethereum*, dan kriptografi lanjutan yang belum cukup.	Menjawab keterbatasan *Ethereum* & IPFS dengan *Hybrid Model* + *Polygon* PoS yang lebih efisien dan mudah diadopsi.
Blockchain Based E-voting System (Nili dkk., 2024)	Sistem *e-voting Blockchain* yang aman, transparan, dan terdesentralisasi untuk integritas hasil *voting* tanpa perantara.	Sistem *e-voting* dengan keamanan *Blockchain*, transparansi, desentralisasi, aksesibilitas, dan efisiensi pemrosesan paralel.	Privasi yang belum detail, skalabilitas tidak teruji, status prototipe, energi/biaya tidak dibahas, dan aspek hukum yang belum dieksplorasi.	Mengisi gap privasi & skalabilitas dengan *Hybrid Model* di *Polygon* PoS, yang lebih efisien dan berorientasi pada prototipe nyata.

Penelitian	Fokus Penelitian	Kelebihan	Keterbatasan (*Gap*)	*Research Gap* yang Diisi Penelitian Ini
Hybrid Voting System Using Blockchain (Nikhare, 2024)	Sistem *voting* hibrida (*Blockchain* + tradisional) untuk otentikasi aman, keandalan, dan peningkatan kepercayaan dalam *voting*.	Sistem *voting* hibrida yang mengintegrasikan metode tradisional dengan *Blockchain* untuk otentikasi kolaboratif, keamanan *voting*, dan peningkatan kepercayaan *voting*.	Penilaian terhadap kelemahan sistem *voting* tradisional dan *Blockchain*, serta usulan model hibrida untuk mengatasi keterbatasan dengan fokus pada keseimbangan keamanan dan kenyamanan.	Menyempurnakan konsep *voting* hibrida dengan penerapan teknis *Hybrid Model* (validasi terpusat + *Blockchain Polygon* PoS) yang seimbang antara efisiensi & transparansi.
A Blockchain Technology Based Voting System (Anand dkk., 2024)	Sistem *e-voting Blockchain* dengan *proof-of-work*, enkripsi El-Gamal, dan ZKP untuk keamanan dan transparansi, yang telah diuji via simulasi dan studi kasus *Rhode Island*.	Sistem *e-voting* dengan audit ketat, verifikasi QR, ZKP, dan PoW, yang telah diuji via simulasi untuk keandalan dan keamanan.	Status prototipe, kompleksitas PoW, desain *Blockchain* berisiko inkonsistensi, serta kurangnya analisis hukum dan peningkatan privasi.	Mengatasi kelemahan PoW (kompleksitas & energi) dengan menggunakan PoS di *Polygon*, serta *Hybrid Model* yang lebih efisien untuk skala organisasi.

Penelitian ini menyoroti bahwa berbagai pendekatan *e-voting* berbasis *Blockchain*, seperti enkripsi hibrida, biometrik, dan *post-quantum cryptography*, masih menghadapi sejumlah tantangan berupa *gas fee* yang tinggi, eksekusi transaksi yang lambat, serta proses validasi identitas yang belum efisien. *Research gap* terletak pada belum adanya model yang mampu menggabungkan validasi terpusat dengan pencatatan hasil *voting* di *Blockchain*, khususnya pada jaringan *Polygon* dengan konsensus *Proof of Stake* (PoS). Penelitian ini mengusulkan *Hybrid Model* yang memanfaatkan keamanan serta transparansi *Blockchain* sekaligus mempertahankan efisiensi sistem terpusat, sehingga proses *e-voting* menjadi lebih aman, transparan, dan efisien.

2.3 Matriks Penelitian

Tabel 2. 3 Matriks Penelitian

Penelitian	*Blockchain Type*	*Smart Contract*	*Hybrid Model*	Keamanan	Konsensus	Implementasi *e-voting*
A Hybrid Proof of Stake-Trust Block Chain Model in Pervasive Social Networking for E-voting System (Ramya dkk., 2022)	*Private-Public*	✓	-	✓	Pos-PoT	✓
Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-voting for National Elections (Daramola, 2020)	*Private*	✓	-	✓	PoC	✓
Blockchain-based Electronic Voting System with Special Ballot and Block Structures that Complies with Indonesian Principle of Voting (Prasetyadi dkk., 2020)	*Private*	-	-	✓	PoW	✓
Decentralized E-voting System Using Blockchain (S.Sekar dkk., 2023)	*Private*	✓	-	✓	PBFT	✓
ELECTRONIC VOTING SYSTEM USING BLOCKCHAIN (Chaithra dkk., 2020)	*Public*	✓	-	✓	PoW	✓
E-voting system using cloud-based Hybrid Blockchain technology (Jayakumari dkk., 2024)	*Private-Public*	✓	-	✓	PBFT	✓
Implementasi Teknologi *Blockchain* dalam Aplikasi *E-voting* Berbasis *Mobile* (Restu Aji & Trisari Harsanti Putri, 2023)	*Private*	✓	-	✓	PoA	✓
Implementation of Decentralized Blockchain E-voting (Khan dkk., 2020)	*Private*	✓	-	✓	PoW	✓
PERANCANGAN *E-VOTING* BERBASIS *SMART CONTRACT* MENGGUNAKAN KEAMANAN ALGORITMA KONSENSUS *PROOF-OF-STAKE* (Lase & Pratiwi, 2020)	*Public*	✓	-	✓	PoS	✓
Penelitian ini	*Public*	✓	✓	✓	PoS	✓

Berdasarkan Tabel 2.3, penelitian yang ditinjau secara keseluruhan telah mengimplementasikan sistem *e-voting* dengan fokus pada aspek keamanan dan penggunaan teknologi *Blockchain*. Setiap penelitian mengadopsi mekanisme konsensus yang berbeda, sesuai

dengan kebutuhan sistem yang diterapkan dan dikembangkan. Beberapa studi juga mengintegrasikan *Smart Contract* untuk meningkatkan efisiensi dan transparansi, serta menerapkan berbagai jenis *Blockchain*, baik *Private*, *Public*, maupun kombinasi *Private-Public*. Sebagian penelitian telah mengadopsi *Hybrid Model* untuk memperkuat keamanan dan integritas data, meskipun jumlahnya masih terbatas. Penelitian ini mengusulkan penerapan sistem *e-voting* berbasis *Blockchain* dengan *Hybrid Model* yang menggabungkan keamanan tinggi, transparansi data, dan efisiensi melalui integrasi *Smart Contract* serta konsensus berbasis *Proof of Stake* (PoS).