IMPLEMENTASI SMART CONTRACT BERBASIS BLOCKCHAIN PADA JARINGAN POLYGON UNTUK PENERBITAN DAN VERIFIKASI SERTIFIKAT

SKRIPSI

ASEP TEGUH HIDAYAT
20210040088

FAKULTAS TEKNIK, KOMPUTER DAN DESAIN
PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS NUSAPUTRA
2025

IMPLEMENTASI SMART CONTRACT BERBASIS BLOCKCHAIN PADA JARINGAN POLYGON UNTUK PENERBITAN DAN VERIFIKASI SERTIFIKAT

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat
Dalam Menempuh Skripsi
Di Program Studi Teknik Informatika

ASEP TEGUH HIDAYAT
20210040088

FAKULTAS TEKNIK, KOMPUTER DAN DESAIN
PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS NUSAPUTRA
2025

DAFTAR ISI

DAFTAR TABEL

No table of figures entries found.

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1PENDAHULUAN

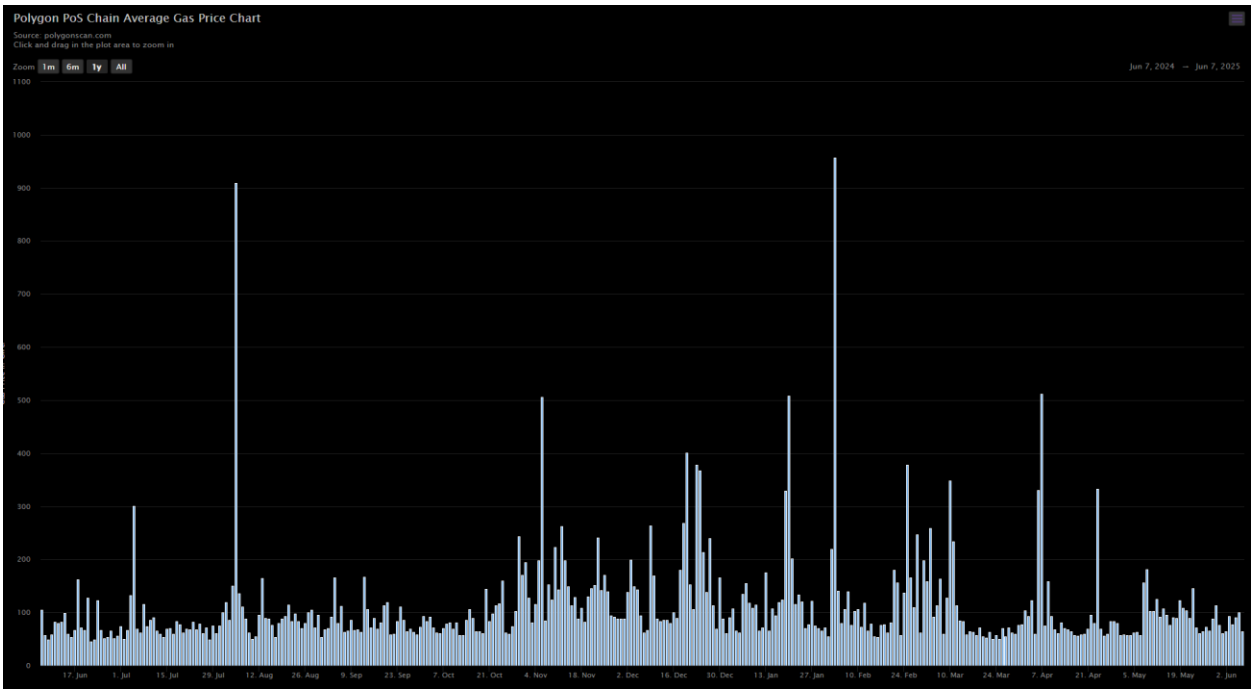
1.1 Latar Belakang

Sertifikat adalah dokumen resmi yang dikeluarkan oleh pihak yang berwenang, yang berfungsi sebagai bukti kepemilikan atau sebagai pernyataan terkait suatu peristiwa[1]. Sertifikat ini menjadi bukti formal dari kompetensi seseorang dan memiliki peran penting dalam berbagai kebutuhan administratif, seperti melamar pekerjaan atau memenuhi persyaratan pendidikan lanjutan. Namun, sistem penerbitan dan verifikasi sertifikat tradisional masih menghadapi sejumlah tantangan, terutama dalam memastikan keaslian dan efisiensi proses verifikasinya[2][3]

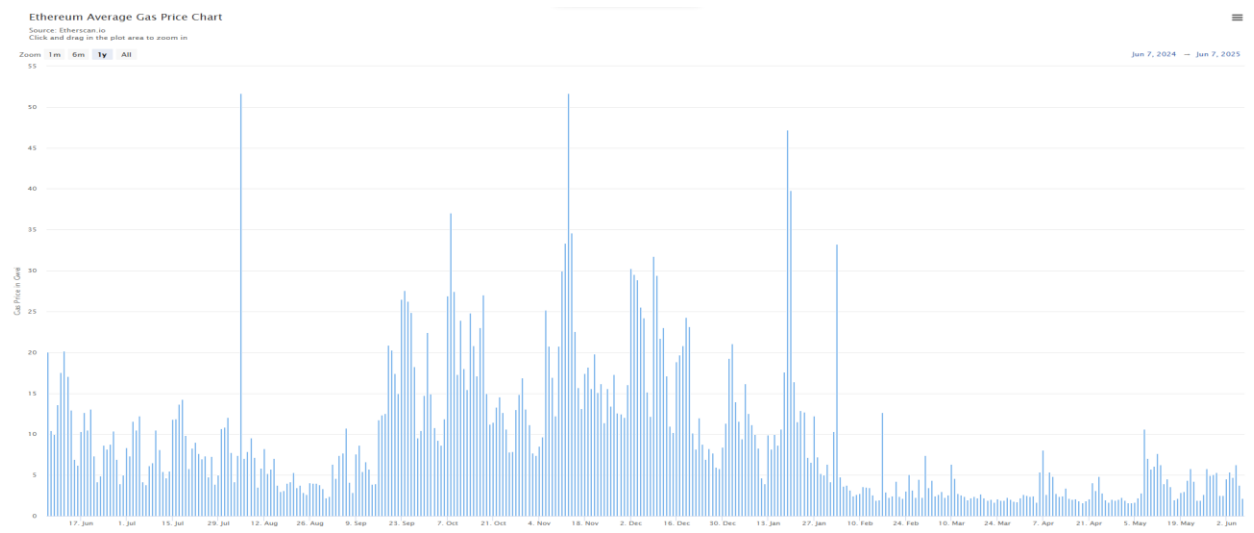
Untuk mengatasi tantangan tersebut, teknologi *blockchain* hadir sebagai solusi inovatif. Blockchain adalah teknologi desentralisasi yang memungkinkan data disimpan secara aman, transparan, dan tidak dapat diubah[4]. Dengan fitur *smart contract*, proses penerbitan dan verifikasi sertifikat dapat dilakukan secara otomatis sesuai aturan yang telah ditentukan. Teknologi ini tidak hanya memastikan keaslian sertifikat, tetapi juga meningkatkan efisiensi dan mengurangi ketergantungan pada sistem terpusat.

Polygon adalah platform blockchain yang sangat potensial untuk aplikasi penerbitan dan verifikasi sertifikat digital karena biaya transaksinya yang jauh lebih rendah. Hal ini sangat kontras dengan Ethereum, yang memiliki biaya transaksi jauh lebih tinggi dan fluktuasi harga gas yang signifikan. Meskipun Ethereum menawarkan keamanan tingkat tinggi, Polygon sebagai solusi

layer-2 tetap memanfaatkan keamanan Ethereum namun dengan efisiensi biaya yang jauh lebih baik, menjadikannya pilihan optimal untuk aplikasi yang sensitif terhadap biaya.



Gambar 1.1 Grafik gas fee rata rata Polygon selama satu tahun



Gambar 1.2 Grafik gas fee rata rata ethereum selama satu tahun

Bulan	Polygon Gwei Rata-rata (Perkiraan)	Polygon Estimasi Biaya (USD)	Ethereum Gwei Rata-rata (Perkiraan)	Ethereum Estimasi Biaya (USD)
Jun 2024	50	0.000219	10	0.52353
Jul 2024	70	0.000307	10	0.52353
Agu 2024	80	0.000350	10	0.52353
Sep 2024	120	0.000525	20	1.04706
Okt 2024	200	0.000875	25	1.308825
Nov 2024	300	0.001312	30	1.57059
Des 2024	250	0.001093	20	1.04706
Jan 2025	400	0.001749	15	0.786045
Feb 2025	250	0.001093	10	0.52353
Mar 2025	150	0.000656	8	0.418824
Apr 2025	100	0.000437	7	0.368361
Mei 2025	80	0.000350	6	0.314196

Table 1 Perbandingan gass fee polygon dan ethereum

Berdasarkan data yang disajikan, terlihat perbandingan biaya gas rata-rata antara Polygon dan Ethereum dari Juni 2024 hingga Mei 2025. Secara umum, biaya gas di Polygon, yang diukur dalam Gwei, menunjukkan fluktuasi yang signifikan dengan puncak pada Januari 2025 sebesar 400 Gwei, dan estimasi biaya dalam USD tetap sangat rendah, selalu di bawah $0.002. Sebaliknya, biaya gas Ethereum, meskipun lebih stabil dalam Gwei (berkisar antara 6 hingga 30 Gwei), memiliki estimasi biaya dalam USD yang jauh lebih tinggi dibandingkan Polygon, berkisar antara

$0.31 hingga $1.57, menegaskan bahwa Ethereum memiliki biaya transaksi yang secara substansial lebih mahal dibandingkan Polygon.

Berdasarkan permasalahan dan potensi yang telah dijelaskan, implementasi smart contract berbasis blockchain pada jaringan Polygon diharapkan dapat menjadi solusi efektif untuk mengatasi risiko pemalsuan dan inefisiensi dalam sistem penerbitan serta verifikasi sertifikat. Dengan memanfaatkan teknologi ini, sertifikat digital dapat diterbitkan dan diverifikasi secara otomatis, aman, dan transparan. Hal ini tidak hanya memberikan perlindungan terhadap integritas data, tetapi juga meningkatkan efisiensi operasional lembaga penerbit sertifikat. Penelitian ini diharapkan dapat menjadi langkah awal untuk mengembangkan sistem sertifikat digital yang lebih modern dan dapat diandalkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, penerbitan dan verifikasi sertifikat yang dilakukan melalui teknologi smart contract pada jaringan Polygon perlu dilakukan pengujian dengan berbagai variabel implementasi untuk mendapatkan solusi terbaik dalam penerbitan dan verifikasi sertifikat yang aman dan efisien. Maka rumusan masalah yang dapat diangkat sebagai berikut:

1. Bagaimana merancang dan mengimplementasikan smart contract pada jaringan Polygon untuk penerbitan dan verifikasi sertifikat?
2. Bagaimana mengintegrasikan Dapp dengan jaringan Polygon untuk memudahkan penerbitan dan verifikasi sertifikat secara terdesentralisasi?
3. Bagaimana Kinerja Jaringan Polygon untuk Penerbitan dan verifikasi Sertifikat?

1.3 Batasan Masalah

Dengan permasalahan yang telah disebutkan, maka kami membatasi masalah yaitu sebagai berikut:

1. Lingkup penelitian ini terbatas pada pengembangan Dapp yang digunakan untuk penerbitan dan verifikasi sertifikat berbasis smart contract di jaringan Polygon, dengan folus pada aplikasi *SAAS(Software As a Service)* penerbitan sertifikat
2. Metode yang digunakan dalam penelitian ini adalah *prototyping*, yang mencakup tahapan perancangan Dapp, pengembangan smart contract pada jaringan Polygon, serta evaluasi sistem berdasarkan fungsionalitas, keamanan, dan usability Dapp yang dikembangkan.

3. Alat Yang digunakan dalam penelitian ini adalah:
    a) Framework pengembangan Dapp berbasis React.js untuk antarmuka pengguna.
    b) Library Ethers.js untuk interaksi dengan jaringan Polygon.
    c) Smart contract yang ditulis menggunakan bahasa Solidity dan di-deploy di jaringan Polygon.
    d) MetaMask sebagai metode autentikasi pengguna untuk berinteraksi dengan blockchain.
    e) Penyimpanan Sertifikat: Mengintegrasikan IPFS (InterPlanetary File System) sebagai media penyimpanan terdesentralisasi untuk sertifikat, sehingga memastikan keamanan dan integritas data.
4. Dalam penelitian ini, standar keamanan yang diterapkan mencakup penggunaan wallet seperti MetaMask untuk verifikasi identitas pengguna. Sertifikat yang diterbitkan akan dicatat di blockchain Polygon dan tidak dapat dimodifikasi, menjamin integritas dan keaslian sertifikat. Proses verifikasi akan dilakukan dengan memeriksa status sertifikat di blockchain.

1.4 Tujuan Penelitian

Dari uraian latar belakang dan rumusan masalah diatas, maka tujuan dari penelitian ini antara lain:

1. Merancang dan mengimplementasikan smart contract untuk penerbitan dan verifikasi sertifikat digital di jaringan Polygon.
2. Mengintegrasikan sistem verifikasi sertifikat berbasis blockchain untuk memastikan keaslian dan integritas data sertifikat yang diterbitkan.
3. Menganalisis kinerja Dapp dalam hal kecepatan dan biaya transaksi untuk penerbitan serta verifikasi sertifikat di jaringan Polygon.

`

1.5 Manfaat Penelitian

Dalam penyusunan dan penulisan yang digunakan oleh penulis, kami menggunakan metode sebagai berikut:

1. Meningkatkan efisiensi dan keamanan dalam penerbitan sertifikat digital. Penelitian ini dapat memberikan solusi untuk meningkatkan efisiensi dalam penerbitan dan verifikasi sertifikat. Dengan menggunakan teknologi blockchain, proses ini dapat dilakukan secara otomatis, aman, dan terdesentralisasi, mengurangi potensi pemalsuan sertifikat dan meningkatkan kepercayaan terhadap sertifikat yang diterbitkan.

2. Menyediakan sistem verifikasi sertifikat yang transparan dan mudah diakses. Penelitian ini memberikan kontribusi pada sistem verifikasi sertifikat yang lebih transparan dan dapat diakses secara mudah oleh semua pihak. Dengan menggunakan Dapp yang terintegrasi dengan blockchain, pengguna dapat memverifikasi keaslian sertifikat tanpa perlu bergantung pada pihak ketiga, meningkatkan kemudahan dan efisiensi dalam verifikasi.

3. Mendorong adopsi teknologi blockchain dalam sektor pendidikan dan profesional. Dengan penerapan sistem verifikasi sertifikat berbasis blockchain, penelitian ini mendorong adopsi teknologi blockchain dalam sektor pendidikan, pelatihan, dan sertifikasi profesional. Hal ini dapat membawa dampak positif bagi pelaku industri yang membutuhkan sistem verifikasi yang lebih aman, efisien, dan terjangkau, serta mendorong inovasi di bidang sertifikasi digital.

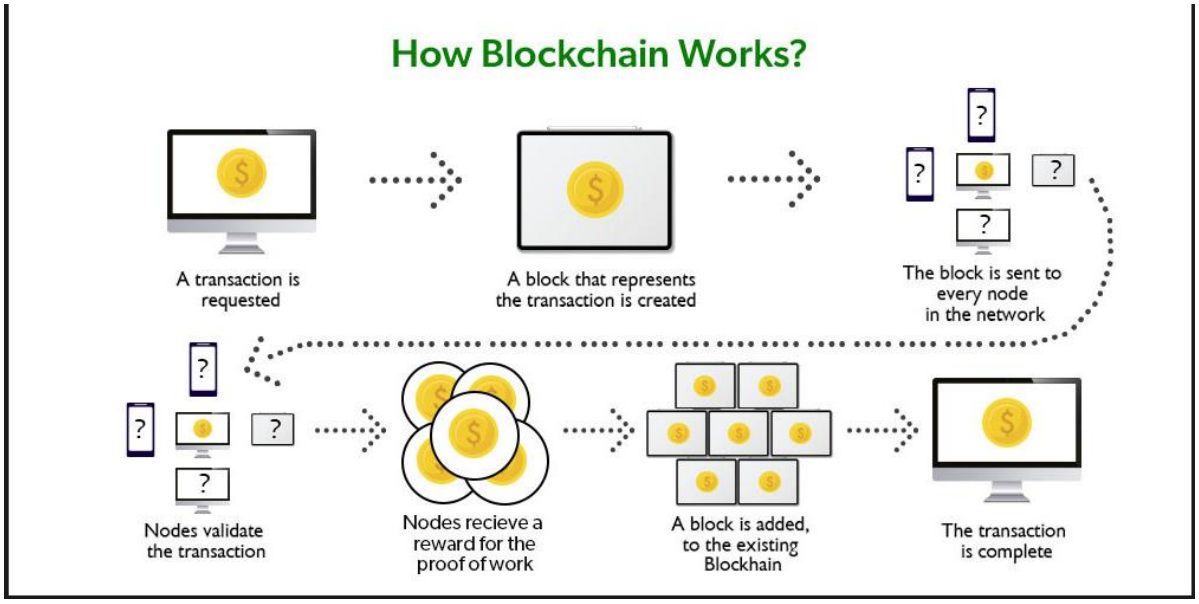
Manfaat penelitian ini memberikan kontribusi pada pengembangan teknologi blockchain dalam konteks praktis, mempermudah proses verifikasi sertifikat, dan meningkatkan transparansi serta keamanan di berbagai sektor.

BAB 2 LANDASAN TEORI

2.1 Landasan Teori

2.1.1 Blockchain

.....**Error! Bookmark not defined.**



Gambar 2.1 Cara Kerja Blockchain

Blockchain merupakan teknologi penyimpanan data yang terdesentralisasi dan aman dalam sebuah jaringan. Teknologi ini memanfaatkan struktur data berbasis blok yang saling terhubung melalui mekanisme kriptografi, memastikan bahwa data yang telah dicatat tidak dapat diubah atau dimanipulasi [4]. Karakteristik utama blockchain yang menjadikannya solusi inovatif untuk pengelolaan data adalah sebagai berikut:

a) Blockchain beroperasi tanpa otoritas pusat yang mengontrol seluruh jaringan. Data disimpan secara terdistribusi di berbagai *node* yang tersebar, menghilangkan ketergantungan pada satu entitas tunggal dan mencegah adanya *single point of failure*.
b) Setiap transaksi dalam blockchain memerlukan proses verifikasi oleh *node-node* dalam jaringan. Proses ini menggunakan mekanisme konsensus, seperti *Proof of Work* (PoW) atau *Proof of Stake* (PoS), untuk memvalidasi data sebelum dicatat. Ditambah dengan penerapan kriptografi, data yang tersimpan terlindungi dari akses atau manipulasi yang tidak sah.

c) Informasi yang tercatat dalam blockchain dapat diakses oleh semua pihak yang memiliki izin akses ke jaringan. Hal ini memungkinkan semua transaksi dapat diaudit secara terbuka, meningkatkan kepercayaan terhadap integritas sistem.

d) Setelah data dicatat dalam blockchain, data tersebut tidak dapat diubah atau dihapus. Setiap blok berisi informasi transaksi yang terhubung secara kriptografis dengan blok sebelumnya, sehingga setiap upaya perubahan akan terdeteksi oleh jaringan dan menjaga integritas historis data secara permanen.

2.1.2 Smart Contract

Gambar 2.2 Cara kerja Smart Contract

Smart contracts adalah protokol digital yang dirancang untuk secara otomatis memfasilitasi, memverifikasi, dan menegakkan perjanjian tanpa memerlukan perantara. Konsep ini pertama kali diperkenalkan oleh Nick Szabo pada tahun 1994 sebagai "protokol transaksi terkomputerisasi yang mengeksekusi ketentuan kontrak" [10], dengan cara menerjemahkan ketentuan kontrak ke dalam kode pemrograman yang disimpan dan dijalankan di jaringan blockchain.

Kelebihan utama smart contract dapat dirangkum sebagai berikut:

a) Otomasi dan Eksekusi Mandiri

Smart contract unggul dalam otomasi dan eksekusi mandiri [11]. Mereka secara otomatis menjalankan perintah berdasarkan logika "jika...maka" yang telah diprogram. Ketika kondisi terpenuhi, transaksi langsung dieksekusi tanpa campur tangan manusia, membuat proses lebih efisien dan terpercaya.

b) Keamanan

Dari sisi keamanan, smart contract memanfaatkan teknologi blockchain yang terdesentralisasi, tidak bergantung pada otoritas pusat [11]. Setiap transaksi tercatat di blok yang saling terhubung dan tersebar di seluruh jaringan, dilindungi oleh kriptografi canggih. Ini menjamin data aman, transparan, dan tidak dapat dimanipulasi, meningkatkan kepercayaan dan mengurangi risiko kesalahan.

c) Transparansi

Transparansi juga menjadi ciri khasnya, karena semua pihak dalam jaringan blockchain memiliki akses penuh terhadap isi dan proses eksekusi smart contract. Setiap transaksi atau perubahan tercatat permanen di blockchain dan dapat dilihat semua peserta, memungkinkan audit terbuka dan verifikasi tanpa perantara.

d) Immutabilitas

Sifat immutabilitas memastikan bahwa setelah diunggah ke blockchain, smart contract menjadi permanen dan tidak dapat diubah atau dihapus oleh siapapun [11]. Struktur kriptografi blockchain menjamin bahwa setiap upaya manipulasi akan terdeteksi dan ditolak oleh jaringan, menciptakan lingkungan yang sangat aman dan bebas dari penipuan.

e) Efisiensi Biaya dan Waktu

Terakhir, smart contract menawarkan efisiensi biaya dan waktu yang signifikan [10]. Dengan menghilangkan kebutuhan akan perantara seperti notaris atau bank, biaya operasional dapat dikurangi secara drastis. Proses eksekusi yang otomatis juga jauh lebih cepat, menghilangkan penundaan manual dan birokrasi, sehingga meningkatkan keandalan dan kecepatan dalam menyelesaikan berbagai jenis transaksi atau kesepakatan.

2.1.3 Polygon

Polygon, sebelumnya dikenal sebagai Matic Network, adalah platform berbasis Ethereum yang dikembangkan untuk mengatasi masalah biaya transaksi yang tinggi dan throughput rendah pada jaringan Ethereum. Dengan menawarkan transaksi yang lebih cepat dan efisien serta biaya gas yang lebih rendah, Polygon menjadi solusi ideal bagi aplikasi terdesentralisasi (DApps) yang membutuhkan pemrosesan data dalam jumlah besar. Platform ini sepenuhnya kompatibel dengan Ethereum, sehingga memungkinkan migrasi dan integrasi DApps dengan mudah[5].

Untuk meningkatkan skalabilitas, Polygon mengadopsi teknologi Layer-2 seperti Plasma Chains, Proof-of-Stake (PoS) sidechains, dan rollups. Teknologi ini memungkinkan pemrosesan transaksi di luar rantai utama Ethereum (off-chain) tanpa mengorbankan keamanan dan desentralisasi. Dengan pendekatan ini, Polygon mampu menangani hingga ribuan transaksi per detik (TPS), jauh melampaui kapasitas Ethereum mainnet. Selain itu, biaya gas yang lebih rendah menjadikannya pilihan menarik bagi pengembang dan pengguna yang ingin mengoptimalkan biaya operasional tanpa kehilangan fungsionalitas.

Keunggulan lain dari Polygon adalah dukungannya terhadap berbagai standar Ethereum, seperti ERC-20 dan ERC-721. Hal ini memungkinkan pengembang untuk memigrasikan DApps dari Ethereum ke Polygon dengan sedikit atau tanpa perubahan pada kode smart contract. Selain itu, Polygon telah menjadi ekosistem bagi berbagai proyek DeFi terkemuka seperti Aave, Curve, dan SushiSwap, serta platform NFT seperti OpenSea, yang memanfaatkan skalabilitas dan efisiensi biaya yang ditawarkan oleh Polygon.

2.1.4 Decentralize Apllication(DAPPS)

DApps, atau aplikasi terdesentralisasi, merupakan aplikasi yang dibangun di atas jaringan blockchain, yang beroperasi tanpa kontrol terpusat. Mereka memanfaatkan teknologi blockchain untuk memberikan transparansi, keamanan, dan ketahanan terhadap sensor. DApps dapat berfungsi di berbagai sektor, termasuk keuangan, manajemen rantai pasokan, dan identitas digital, dengan tujuan untuk meningkatkan integritas data dan mengurangi ketergantungan pada pihak ketiga[6]

2.1.5 Sertifikat

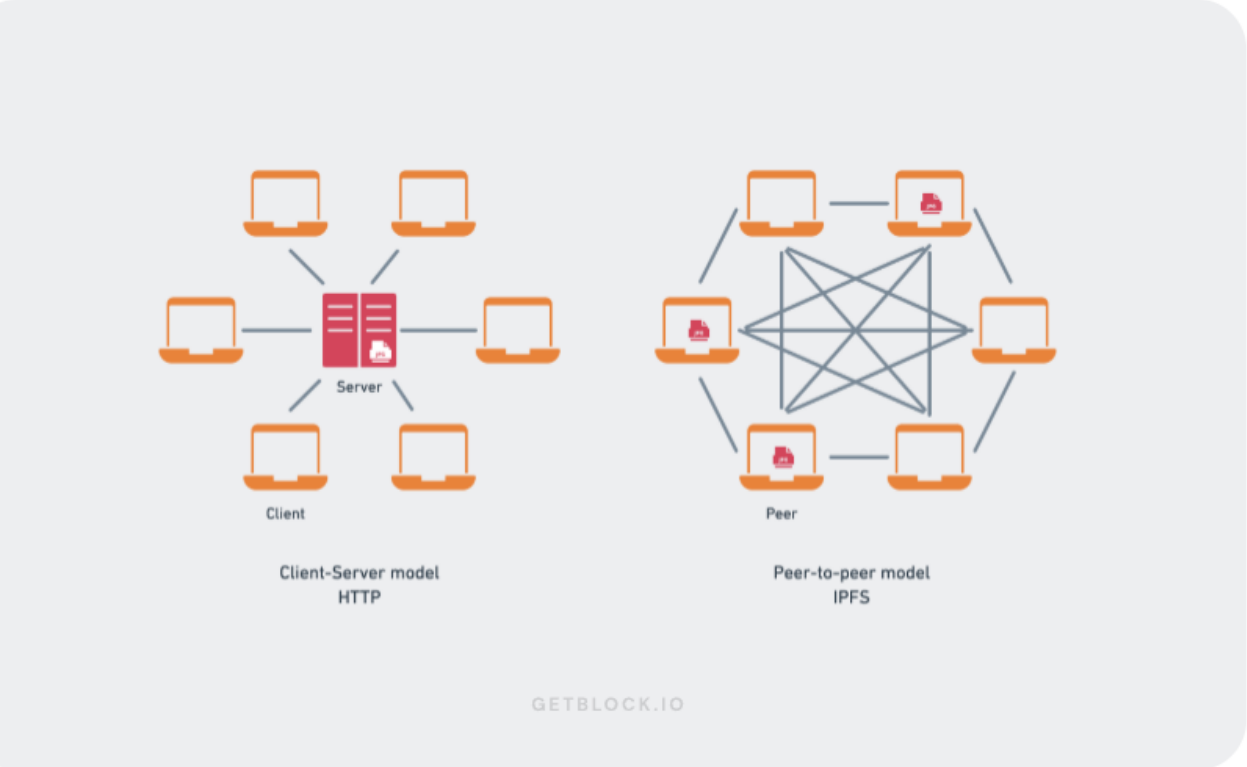
Sertifikat adalah dokumen resmi yang diterbitkan oleh lembaga atau institusi yang memiliki otoritas, berfungsi sebagai bukti kepemilikan atau pencapaian tertentu. Sertifikat diberikan setelah individu menyelesaikan program, kursus, atau pelatihan, menunjukkan bahwa individu tersebut telah memenuhi syarat atau kompetensi yang ditetapkan.

Secara umum, sertifikasi memiliki beberapa tujuan dan manfaat penting. Dalam konteks pendidikan, sertifikasi berperan dalam peningkatan kualitas guru dan tenaga pendidik lainnya, sesuai standar kompetensi yang ditetapkan, sebagaimana diatur dalam Undang-Undang

Republik Indonesia Nomor 14 Tahun 2005 tentang Guru dan Dosen. Selain itu, sertifikat berfungsi sebagai validasi formal atas keahlian dan kompetensi seseorang dalam bidang tertentu, menjadikannya faktor penting dalam proses rekrutmen di dunia kerja. Memiliki sertifikat juga dapat meningkatkan daya saing individu di pasar kerja yang kompetitif, menunjukkan komitmen terhadap pengembangan diri serta kepemilikan keterampilan yang diakui secara resmi.

Di samping fungsi-fungsi tersebut, sertifikat juga berperan sebagai alat bukti hukum yang kuat. Sebagai contoh, dalam konteks hukum pertanahan, sertifikat hak milik atas tanah memberikan kepastian hukum kepada pemegangnya. Menurut penelitian, sertifikat memiliki kekuatan hukum yang mengikat dan menjadi acuan utama dalam penyelesaian sengketa tanah Data fisik dan yuridis yang tercantum dalam sertifikat dianggap sah selama tidak ada bukti sebaliknya.

2.1.6 IPFS (Inter Planetary File System)



Gambar 2.3 perbedaan ipfs dengan http

IPFS (InterPlanetary File System) adalah sebuah protokol penyimpanan dan distribusi file yang terdesentralisasi. Berbeda dengan sistem penyimpanan tradisional yang menggunakan model berbasis lokasi (location-based), IPFS menggunakan model berbasis konten (content-based). Artinya, setiap file atau data di IPFS diidentifikasi oleh hash unik yang dihasilkan dari kontennya sendiri, bukan oleh lokasi penyimpanannya. Hal ini memungkinkan file untuk diakses secara efisien dan aman, terlepas dari di mana file tersebut disimpan.

Salah satu keunggulan utama IPFS adalah kemampuannya dalam menyimpan data secara terdesentralisasi. File yang diunggah ke IPFS akan dipecah menjadi beberapa bagian kecil (chunks) dan didistribusikan ke berbagai node di jaringan. Setiap node yang menyimpan bagian dari file tersebut dapat berperan sebagai penyedia data, sehingga tidak ada ketergantungan pada satu server pusat. Ini membuat IPFS sangat tahan terhadap kegagalan server (fault-tolerant) dan serangan DDoS (Distributed Denial of Service).

2.2 Penelitian Terkait

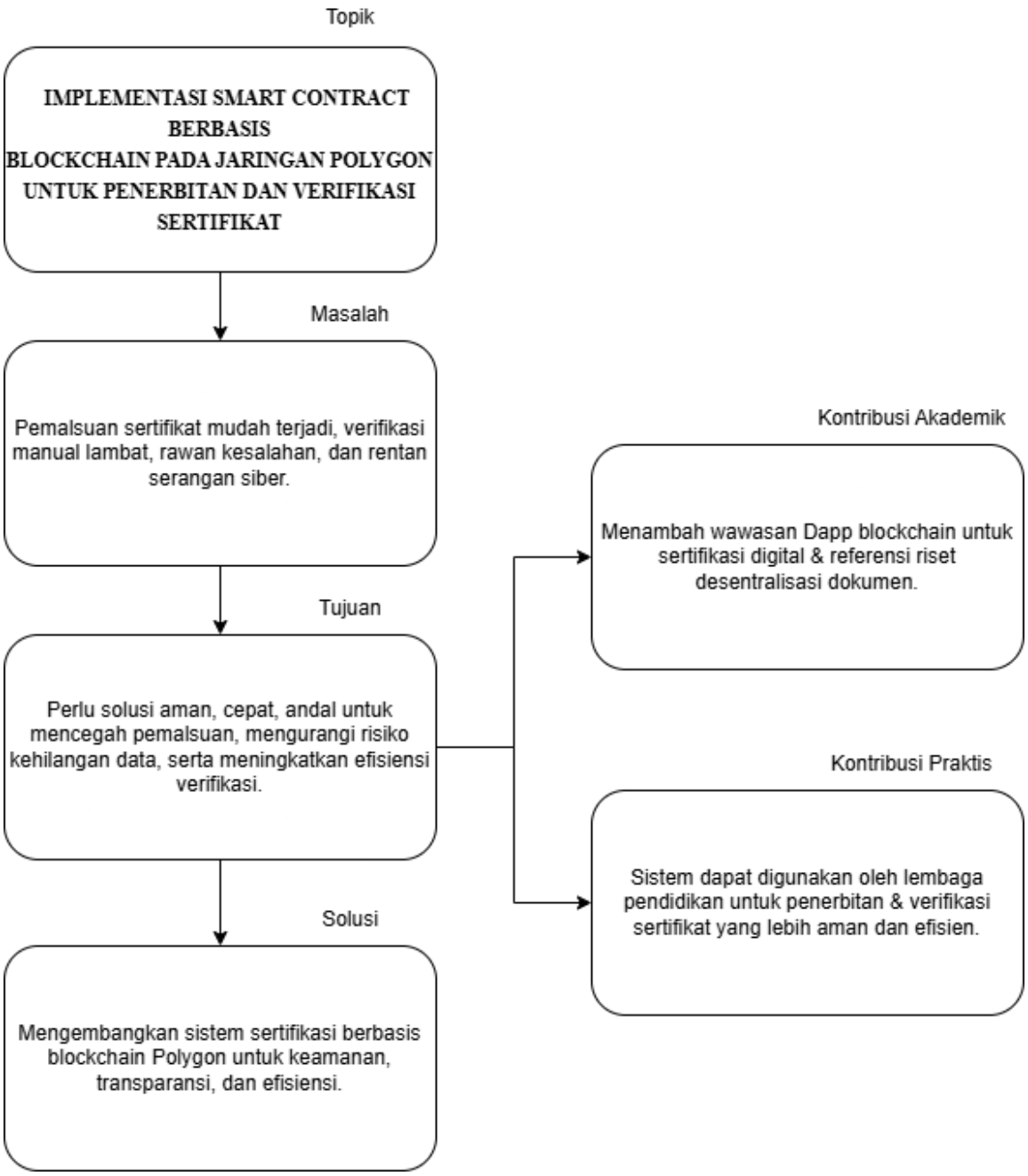
No	Peneliti dan tahun Peneliti	Judul	Hasil	Persamaan	Perbedaan
1	Ravi Singh Lamkoti, Devdoot Maji, Hitesh Shetty, Prof. Bharati Gondhalekar 2021	Certificate Verification using Blockchain and Generation of Transcript[7]	Sistem ini menghasilkan solusi pembuatan dan validasi sertifikat digital yang aman dan efisien, dengan hash unik tersimpan di blockchain Ethereum, dokumen asli di IPFS, validasi melalui perbandingan hash menggunakan ID unik atau dokumen, didukung smart contract	Memiliki alur aplikasi yang sama, dengan teknologi yang digunakan hampir sama seperti penggunaan smart contract, ipfs, ether.js dan	Perbedaan terletak pada jaringan yang digunakan penelitian ini menggunakan jaringan layer 1 etherium sedangkan penulis menggunakan layer 2 poligon

			Solidity, Metamask, Ganache, dan Truffle.	output yang sama	
2	Heri Wijayanto, Pangeran Muhammad Waliyullah 2024	Aplikasi Verifikasi Sertifikat Berbasis Website Menggunakan Blockchain	Jurnal ini membahas aplikasi verifikasi sertifikat berbasis website menggunakan blockchain Ethereum untuk mencegah pemalsuan. Aplikasi ini mendukung pembuatan, penerbitan, pencarian, dan validasi sertifikat digital dengan smart contract Solidity, algoritma hash SHA-256, Truffle, Ganache, Flask, dan Web3.js. Pengujian black box menunjukkan semua fitur berfungsi dengan baik. [7]	Persamaan ada pada alur dan fitur aplikasi yang mana mampu untuk menerbitkan dan memverifikasi keaslian melalui file sertifikat	Pengembangan aplikasi pada jurnal ini menggunakan truffle sedangkan penulis menggunakan hardhat penulis juga memanfaatkan decentralize storage sedangkan jurnal ini tidak
3	Windra Swastika, Hermawan Wira Santoso , Oesman Hendra Kelana 2022[9]	Rancang Bangun Website Akademik Dengan Penyimpanan Sertifikat Digital Menggunakan	Jurnal ini membahas website akademik untuk penyimpanan sertifikat digital berbasis blockchain Ethereum dan Geth, menggunakan smart contract untuk keamanan dan pencegahan pemalsuan. Sistem memproses 200	Penelitian ini sama sama mempunyai output untuk menerbitkan sertifikat yang disimpan pada jaringan blockchain	Penelitian ini menggunakan blockchain lokal dan berfokus pada penerbitan sertifikat pasca-kursus, sementara penelitian

		Teknologi Blockchain	transaksi dalam 8 detik, membutuhkan 22.6 GB untuk 10 juta blok, aman dari penerbitan ilegal dan perubahan tidak sah, serta mendukung fitur melihat, membeli kelas, menerbitkan, dan memverifikasi sertifikat. [10]		penulis hanya menekankan penerbitan dan verifikasi sertifikat.
4	Seni Oknora Firza, Yuhandri Sumijan 2024	Teknologi Blockchain dalam Keamanan Sertifikat Menggunakan Smart Contracts dan Distributed Ledger pada Platfrom Edutech	Penelitian ini menunjukkan teknologi Blockchain dengan Smart Contracts dan Distributed Ledger efektif meningkatkan keamanan sertifikat pada platform Edutech, mengotomatiskan verifikasi, mencegah pemalsuan, dan meningkatkan transparansi. IPFS menjamin keaslian data, dengan enkripsi SHA-256 memastikan validasi cepat. Blockchain juga berpotensi untuk sistem	Memiliki tujuan yang sama yaitu membuat system sertifikat di jaringan blockchain	Pada jurnal ini tidak disebutkan fitur fitur yang digunakan hanya menyimpulkan bahwa bisa dilakukan sedangkan yang dibuat penulis lebih rinci mulai dari alur pada blockchain hingga decentralize storage

			akademik, jaringan sensor, dan e-voting. [11]		

2.3 Kerangka Berfikir

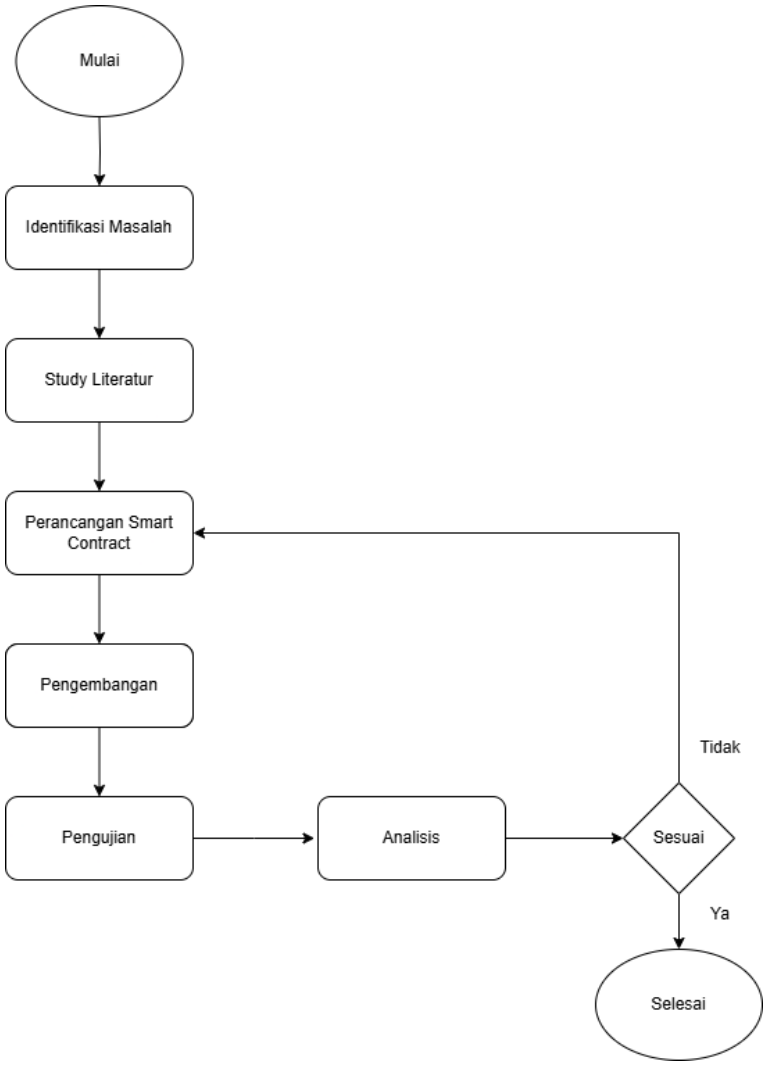


Gambar 2.4 Kerangka berfikir

kerangka berpikir diatas menjadi dasar untuk mengatasi masalah ketika mengembangkan system penerbitan dan verifikasi sertifikat pada jaringan blockchain. Ini menunjukkan bagaimana identifikasi masalah, urgensi, tujuan, solusi, serta hasil yang diharapkan untuk memudahkan proses penerbitan dan verifikasi sertifikat, selain itu membuat system lebih aman dari berbagai masalah

BAB 3 METODE PENELITIAN

3.1 Metode Penelitian



Gambar 3.1 Diagram Metode Berfikir

Dalam melaksanakan penelitian ini, penulis memutuskan untuk menggunakan pendekatan yang terstruktur. Prosesnya dimulai dengan menetapkan fondasi yang kuat, yaitu memahami dan merumuskan inti permasalahan yang akan diteliti. Ini mencakup menjelaskan alasan di balik penelitian, merumuskan pertanyaan-pertanyaan utama, dan menetapkan apa yang ingin dicapai, memastikan seluruh upaya penelitian memiliki fokus yang jelas.

Setelah masalah berhasil ditetapkan, langkah selanjutnya adalah memperkaya pemahaman melalui penelusuran berbagai informasi dan karya-karya sebelumnya yang relevan. Tahap ini membantu penulis membangun kerangka pengetahuan yang kuat, melihat bagaimana topik serupa telah ditangani, dan menemukan peluang untuk memberikan kontribusi baru dalam penelitian ini.

Berbekal pemahaman dari studi literatur dan identifikasi masalah, penelitian berlanjut ke tahap perancangan. Pada fase ini, penulis mulai merancang detail solusi, termasuk bagaimana sistem akan bekerja secara keseluruhan, arsitektur sistem, rancangan *smart contract* akan diatur, dan bagaimana pengguna akan berinteraksi dengannya. Perancangan ini memastikan bahwa solusi yang dikembangkan dapat mengatasi masalah yang telah diidentifikasi dan sesuai dengan kebutuhan yang ada.

Setelah rancangan selesai, tibalah saatnya untuk tahap pengembangan. Di sini, *smart contract* dibangun menggunakan bahasa pemrograman yang sesuai dan diintegrasikan dengan *platform blockchain* yang dipilih. Selain itu, bagian antarmuka yang akan digunakan pengguna juga dibuat, memungkinkan mereka berinteraksi dengan sistem secara lancar.

Tahap berikutnya merupakan fase krusial yang melibatkan pengujian langsung pada jaringan Polygon Testnet. Pengujian ini dirancang untuk mensimulasikan transaksi dalam kondisi yang menyerupai lingkungan operasional sebenarnya. Pemilihan Polygon sebagai *platform* utama didasari oleh efisiensi biaya transaksi yang signifikan. Fokus utama pengujian ini adalah memvalidasi kinerja *Smart Contract* yang diimplementasikan, khususnya melalui pengukuran total *gas fee* yang dikeluarkan selama proses penerbitan dan verifikasi sertifikat. Apabila *gas fee* yang dikeluarkan terbukti efisien sesuai harapan, ini akan mengindikasikan bahwa *Smart Contract* yang dirancang telah berhasil mencapai tujuan penelitian, yaitu terwujudnya solusi yang aman dan efisien untuk penerbitan dan verifikasi sertifikat digital. Berikut adalah penjelasan lebih lanjut mengenai metode penelitian dan metode pengembangan perangkat lunak yang diterapkan:

3.1.1 Metode Kuantitatif

Metode penelitian kuantitatif adalah pendekatan yang melibatkan pengumpulan dan analisis data numerik dengan kontrol variabel [12]. Pendekatan ini dipilih untuk secara objektif

menguji hipotesis melalui data yang terukur, sehingga menghasilkan kesimpulan yang terstruktur dan dapat diverifikasi ulang.

Dalam penelitian ini, metode kuantitatif memegang peran penting dalam mengukur efisiensi *gas fee* dan kecepatan transaksi pada *smart contract* untuk penerbitan dan verifikasi sertifikat di jaringan Polygon. Data akan diperoleh melalui serangkaian pengujian *smart contract* dalam berbagai skenario penggunaan, dan kemudian dianalisis secara statistik untuk mengkonfirmasi *gas fee* serta waktu proses yang efisien. Data ini dapat berasal dari observasi langsung terhadap perilaku *smart contract* di Polygon Testnet atau dari studi literatur terkait performa jaringan blockchain. Hasil numerik yang diperoleh akan menjadi dasar kuat untuk menilai efektivitas implementasi *smart contract* yang dikembangkan, sejalan dengan tujuan penelitian untuk mendapatkan solusi terbaik dalam penerbitan dan verifikasi sertifikat yang aman dan efisien.

3.1.2 Metode Prototyping

Metode *prototyping* adalah bagian dari *Software Development Lifecycle* (SDLC) yang diadopsi dalam penelitian ini untuk mengembangkan dan menguji *smart contract* yang ditujukan untuk penerbitan dan verifikasi sertifikat digital. Sebuah *prototype* merupakan versi awal dari sistem perangkat lunak yang berfungsi sebagai representasi ide, alat eksperimen desain, serta sarana untuk mengidentifikasi dan menyelesaikan masalah [13]. *Prototyping* memungkinkan pengembangan solusi yang bersifat iteratif, di mana setiap siklus menghasilkan versi yang lebih baik berdasarkan hasil pengujian dan evaluasi. Pendekatan ini sangat sesuai untuk penelitian yang melibatkan pengembangan teknologi baru atau kompleks, seperti implementasi *smart contract* pada jaringan blockchain.

Proses *prototyping* dimulai dengan identifikasi kebutuhan secara mendalam, yaitu menentukan kebutuhan fungsional dan non-fungsional untuk *smart contract* penerbitan dan verifikasi sertifikat. Fokus utama adalah mengidentifikasi fungsionalitas esensial seperti kemampuan penerbitan dan verifikasi sertifikat, serta bagaimana mengoptimalkan operasi ini di jaringan Polygon dengan mempertimbangkan efisiensi biaya transaksi. Tahap ini juga mencakup pemahaman mendalam tentang struktur *gas fee* di Polygon dan strategi untuk merancang *smart contract* agar mencapai efisiensi biaya dan kecepatan transaksi, sejalan dengan rumusan masalah mengenai kinerja jaringan.

Setelah kebutuhan berhasil diidentifikasi, tahap perancangan awal dilakukan. Pada fase ini, arsitektur *smart contract* didesain, mempertimbangkan fungsi-fungsi penerbitan dan verifikasi sertifikat, serta bagaimana *smart contract* akan terintegrasi dengan antarmuka pengguna (DApp) dan sistem penyimpanan terdesentralisasi.

3.2 Identifikasi Masalah

Berdasarkan latar belakang dan rumusan masalah yang telah diuraikan sebelumnya, penelitian ini berupaya untuk mengatasi beberapa permasalahan utama terkait implementasi *smart contract* berbasis *blockchain* Polygon untuk penerbitan dan verifikasi sertifikat digital.

Pertama, mengenai bagaimana merancang dan mengimplementasikan *smart contract* pada jaringan Polygon untuk penerbitan dan verifikasi sertifikat. Sistem konvensional dalam penerbitan sertifikat masih sangat bergantung pada otoritas terpusat, yang rentan terhadap pemalsuan dan manipulasi data. Oleh karena itu, melalui penggunaan *smart contract* pada jaringan Polygon, diharapkan sistem yang dikembangkan dapat menjamin integritas dan keaslian sertifikat secara transparan dan aman, mengurangi risiko yang ada pada sistem terpusat. Konsep ini didukung oleh model *Software as a Service* (SaaS) yang memungkinkan berbagai individu atau organisasi untuk berperan sebagai penerbit, sehingga mendemokratisasi proses penerbitan sertifikat tanpa ketergantungan pada satu otoritas tunggal.

Kedua, permasalahan berfokus pada bagaimana mengintegrasikan *Decentralized Application* (DApp) dengan *blockchain* Polygon untuk memudahkan penerbitan dan verifikasi sertifikat secara terdesentralisasi. Proses verifikasi sertifikat secara tradisional sering kali memerlukan validasi dari pihak ketiga, yang berpotensi memperlambat proses dan meningkatkan risiko kesalahan. Dengan adanya DApp yang terhubung langsung dengan *smart contract*, pengguna diharapkan dapat melakukan penerbitan dan verifikasi sertifikat dengan mudah tanpa memerlukan perantara, sehingga meningkatkan efisiensi dan aksesibilitas.

Ketiga, penelitian ini juga akan menjawab bagaimana kinerja jaringan Polygon untuk penerbitan dan verifikasi sertifikat. Implementasi *smart contract* di *blockchain* seringkali menghadapi tantangan seperti biaya transaksi (*gas fee*), keamanan kontrak, dan efisiensi

penyimpanan data. Oleh karena itu, penelitian ini akan mengidentifikasi dan mencari solusi atas tantangan-tantangan tersebut agar sistem dapat beroperasi secara optimal, sejalan dengan tujuan untuk mencapai penerbitan dan verifikasi sertifikat yang efisien.

Berdasarkan permasalahan-permasalahan yang telah dijelaskan, penelitian ini mengusulkan pengembangan sebuah sistem penerbitan dan verifikasi sertifikat yang memanfaatkan *blockchain* dan *smart contract* pada jaringan Polygon. Dengan pendekatan ini, sistem yang dikembangkan diharapkan dapat menjadi solusi yang lebih aman, efisien, dan transparan dalam pengelolaan sertifikat digital, terutama dengan kapabilitasnya sebagai *platform SaaS* yang memungkinkan berbagai pihak untuk menjadi penerbit sertifikat.

3.3 Studi Literatur

Tahap studi literatur dalam penelitian ini berfokus pada pendalaman pemahaman mengenai penerapan *smart contract* dalam sistem penerbitan dan verifikasi sertifikat berbasis *blockchain* di jaringan Polygon. Tujuan utamanya adalah untuk mengeksplorasi secara komprehensif keunggulan serta tantangan yang muncul dalam implementasi *smart contract* guna memastikan keaslian dan keamanan sertifikat digital.

Beberapa referensi relevan menunjukkan bahwa *smart contract* memiliki potensi besar dalam hal efisiensi dan keamanan. Penelitian oleh Laila Alfina Mayasari Rizki dan Dedi Farera Prasetya [13] menjelaskan bahwa sifat *self-executing* dari *smart contract* menjamin keamanan data dan terlaksananya isi perjanjian secara otomatis ketika kondisi yang ditentukan terpenuhi. Studi tersebut juga mengindikasikan bahwa sistem verifikasi dokumen yang terintegrasi dengan *smart contract* telah terbukti mampu meningkatkan efisiensi proses pelacakan dan verifikasi dokumen, sekaligus menjaga kerahasiaan informasi sensitif.

Implementasi *smart contract* pada jaringan Polygon menawarkan beberapa keunggulan signifikan. Polygon dikenal mampu memproses transaksi dengan kecepatan tinggi dan biaya yang relatif lebih rendah dibandingkan jaringan *blockchain* lainnya [14]. Selain itu, pemanfaatan teknologi *Zero-Knowledge Proofs* (ZKP) yang diterapkan dalam beberapa konteks *blockchain* memungkinkan verifikasi keaslian dokumen tanpa perlu mengungkapkan informasi yang bersifat rahasia [15]. Penggunaan jaringan Polygon dengan protokol konsensus *Proof of Stake* (PoS) juga

berkontribusi pada proses verifikasi dokumen yang lebih cepat, hemat biaya, dan dapat diakses secara luas.

Hasil dari studi literatur ini memberikan fondasi pemahaman yang kuat mengenai potensi penggunaan *smart contract* dalam sistem sertifikat digital. Sistem yang dikembangkan diharapkan tidak hanya meningkatkan keamanan proses pelacakan dokumen dengan tidak menguak isi dokumen yang bersifat rahasia dan dilindungi oleh undang-undang [15], tetapi juga dapat meningkatkan integritas data. Melalui pengembangan lebih lanjut, sistem ini memiliki potensi untuk diintegrasikan dengan sistem manajemen dokumen yang lebih luas, sehingga memperkuat efisiensi dan efektivitas proses verifikasi secara keseluruhan [15].

3.4 Perancangan Sistem

Perancangan sistem dalam penelitian ini merupakan langkah krusial untuk memastikan bahwa sistem penerbitan dan verifikasi sertifikat berbasis *blockchain* dapat berfungsi secara optimal, aman, dan efisien. Tahap perancangan ini mencakup analisis kebutuhan fungsional dan non-fungsional, desain arsitektur sistem secara keseluruhan, perancangan *smart contract*, serta desain antarmuka pengguna yang intuitif.

3.4.1 Analisis Kebutuhan

Analisis kebutuhan dilakukan untuk mengidentifikasi dan menentukan fitur-fitur esensial yang diperlukan dalam pengembangan sistem. Berdasarkan tujuan penelitian, fitur-fitur utama yang akan dikembangkan meliputi:

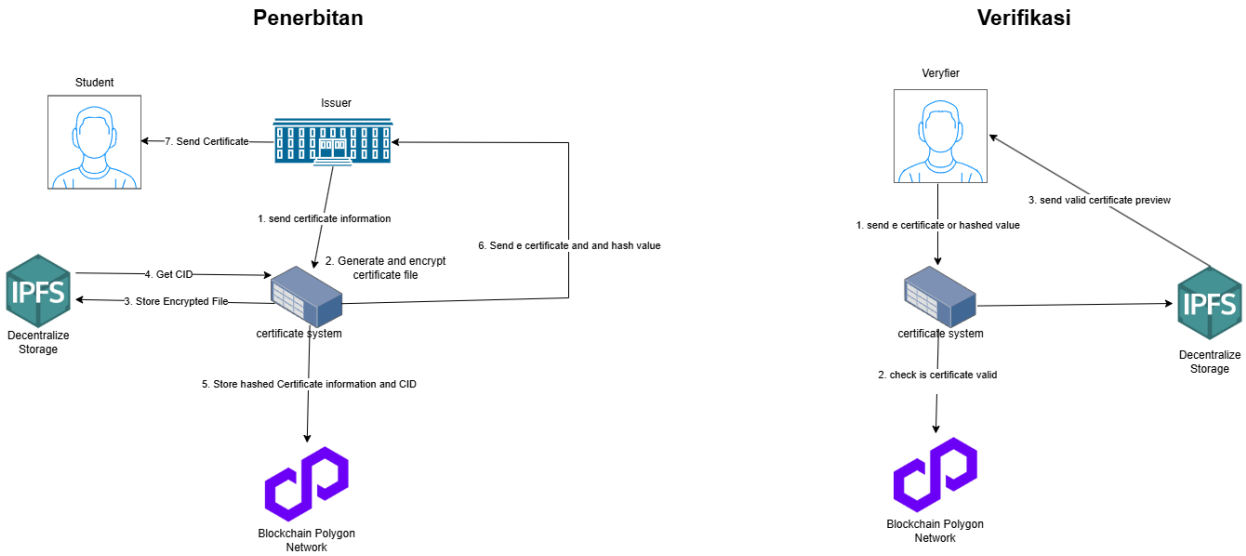
a) Sistem harus mampu menerbitkan sertifikat digital secara otomatis melalui *smart contract*, dengan data yang disimpan secara aman dan tidak dapat diubah (*immutable*) di *blockchain*.
b) Sistem wajib menyediakan mekanisme yang transparan dan terdesentralisasi untuk verifikasi keaslian sertifikat oleh penerima atau pihak ketiga, memastikan proses yang mudah diakses dan memberikan kepastian validitas.
c) Sistem perlu menyediakan fungsionalitas untuk mencabut sertifikat yang telah diterbitkan, dengan batasan bahwa hanya pihak penerbit yang berwenang yang memiliki hak untuk melakukannya.

d) Data sertifikat harus disimpan secara terdesentralisasi menggunakan teknologi *blockchain*, diintegrasikan dengan *InterPlanetary File System* (IPFS) untuk menjamin keamanan dan integritas dokumen.

e) Sistem harus dilengkapi dengan antarmuka pengguna (*User Interface*) yang ramah bagi penerbit maupun penerima sertifikat, serta mendukung interaksi mulus dengan *smart contract* melalui *wallet* populer seperti MetaMask.

3.4.2 Desain Arsitektur Sistem

Arsitektur sistem dirancang secara komprehensif untuk memastikan bahwa semua komponen dapat bekerja secara terintegrasi dan optimal. Gambaran umum arsitektur sistem yang akan diimplementasikan dapat dilihat pada gambar di bawah ini, yang menunjukkan alur kerja antara komponen dan interaksi dua peran pengguna utama, yaitu *issuer* (pihak penerbit) dan *verifier* (pihak verifikasi).



Sistem ini melibatkan beberapa komponen utama:

a) *Smart Contract* yang bertanggung jawab penuh untuk menerbitkan, memverifikasi, dan mencabut sertifikat digital.

b) Jaringan Polygon yang berfungsi sebagai *platform blockchain* utama, menyediakan infrastruktur terdesentralisasi untuk menjalankan *smart contract* dan mencatat semua transaksi sertifikat.

c) Antarmuka Pengguna (*Decentralized Application* / DApp) yang bertindak sebagai *frontend* aplikasi, memungkinkan pengguna (baik penerbit maupun verifikator) untuk berinteraksi secara mudah dengan sistem.
d) *InterPlanetary File System* (IPFS) yang digunakan sebagai sistem penyimpanan terdesentralisasi untuk menyimpan dokumen sertifikat yang berukuran lebih besar, memastikan ketersediaan dan integritas data.

Alur kerja sistem dirancang dengan langkah-langkah yang jelas. Penerbit sertifikat memulai proses dengan memasukkan data melalui antarmuka pengguna. Data ini kemudian dikirim ke *smart contract* untuk dicatat dan diamankan di *blockchain* Polygon. Selanjutnya, penerima sertifikat atau pihak ketiga dapat dengan mudah memverifikasi keaslian sertifikat melalui antarmuka pengguna. Proses ini diakhiri dengan *smart contract* yang memvalidasi data sertifikat yang diminta dan memberikan hasil verifikasi secara transparan.

3.4.3 Desain Smart Contract

Smart contract merupakan inti fungsional dari sistem ini. Keberadaannya sangat esensial karena menjadi fondasi utama yang memungkinkan seluruh proses penerbitan dan verifikasi sertifikat berjalan secara otomatis, transparan, dan aman di atas jaringan *blockchain*. Dirancang dengan detail, *smart contract* ini berperan sebagai protokol digital yang mengeksekusi ketentuan-ketentuan yang telah diprogram tanpa memerlukan intervensi pihak ketiga, sehingga memastikan integritas dan keandalan data sertifikat.

Rancangan *smart contract* ini memiliki fungsi-fungsi utama:

- Fungsi issueCertificate bertujuan untuk menerbitkan sertifikat baru, memastikan data yang relevan dicatat secara permanen dan aman di *blockchain*.
- Fungsi verifyCertificate memungkinkan validasi keaslian sertifikat dengan membandingkan data yang diserahkan dengan catatan yang tersimpan di *blockchain*.
- Fungsi revokeCertificate disediakan untuk pembatalan sertifikat yang telah diterbitkan sebelumnya, jika diperlukan.

3.4.4 Desain Antarmuka Pengguna

Antarmuka pengguna didesain secara spesifik untuk memfasilitasi interaksi yang intuitif dan efisien antara pengguna dengan sistem. Desain ini bertujuan untuk menciptakan pengalaman yang mulus bagi seluruh pihak yang terlibat, baik penerbit maupun penerima sertifikat, memastikan bahwa proses pengelolaan sertifikat digital dapat dilakukan dengan mudah dan tanpa hambatan teknis yang berarti.

Desain antarmuka pengguna ini mencakup beberapa fitur utama yang dirancang untuk mendukung berbagai kebutuhan pengguna dalam pengelolaan sertifikat digital. Fitur-fitur ini secara kolektif memungkinkan alur kerja yang komprehensif, mulai dari tahap penerbitan hingga proses verifikasi sertifikat, memastikan bahwa setiap interaksi pengguna dengan sistem berlangsung secara efektif dan efisien. Fitur-fitur tersebut adalah sebagai berikut:

a) Halaman Penerbitan Sertifikat memfasilitasi penerbit untuk memasukkan data sertifikat dan secara langsung menerbitkannya melalui *smart contract*.
b) Halaman Verifikasi Sertifikat memungkinkan penerima atau pihak ketiga untuk melakukan verifikasi keaslian sertifikat dengan mudah.
c) Halaman Riwayat Sertifikat berfungsi untuk menampilkan daftar komprehensif dari semua sertifikat yang telah diterbitkan atau diverifikasi.

Adapun teknologi yang digunakan dalam pengembangan antarmuka ini dipilih secara cermat untuk memastikan kinerja optimal, responsivitas, dan keamanan dalam berinteraksi dengan *blockchain* Polygon. Pemilihan teknologi ini didasarkan pada kapabilitasnya dalam mendukung aplikasi terdesentralisasi (*DApp*) yang handal dan memberikan pengalaman pengguna yang unggul, sekaligus menjaga integritas data di lingkungan *blockchain*. Teknologi-teknologi tersebut meliputi:

a) *Frontend* yang dibangun menggunakan *framework* React.js bertujuan untuk menciptakan antarmuka yang interaktif dan responsif, memastikan sistem dapat diakses dengan baik di berbagai perangkat.
b) Integrasi dengan *blockchain* menggunakan *library* Ethers.js berfungsi untuk menghubungkan antarmuka pengguna dengan *smart contract* yang beroperasi di jaringan Polygon, memfasilitasi komunikasi data yang aman dan terdesentralisasi.

c) Integrasi *wallet* melalui MetaMask yang berfungsi sebagai metode autentikasi utama bagi pengguna untuk berinteraksi secara aman dengan *blockchain*, memberikan kemudahan akses tanpa mengorbankan kontrol atas aset digital pengguna.

3.5 Pengembangan Sistem

Tahap pengembangan sistem merupakan fase krusial yang dilaksanakan setelah seluruh proses perancangan sistem rampung. Pada tahapan ini, rancangan konseptual yang telah dibuat akan diimplementasikan menjadi sebuah sistem yang fungsional dan siap diuji. Proses pengembangan ini memastikan bahwa setiap komponen sistem dibangun sesuai dengan spesifikasi desain, mengintegrasikan berbagai teknologi yang diperlukan untuk mewujudkan sistem penerbitan dan verifikasi sertifikat berbasis *blockchain* yang efektif dan efisien. Fokus utama pada tahap ini adalah menerjemahkan desain arsitektur, *smart contract*, dan antarmuka pengguna ke dalam kode program yang bekerja secara harmonis, sekaligus mengatasi tantangan teknis yang mungkin muncul selama proses implementasi. Ini adalah fase di mana teori diubah menjadi praktik, menciptakan fondasi operasional dari solusi yang diusulkan.

3.5.1 Pengembangan Smart Contract

Smart contract merupakan inti fungsional dari sistem ini. Proses pengembangannya dilakukan dengan menggunakan bahasa pemrograman Solidity dan akan di-*deploy* pada jaringan Polygon. Pengembangan ini melibatkan beberapa langkah krusial:

a) Penulisan Kode Smart Contract *Smart contract* ini dikembangkan dengan mengintegrasikan fungsi-fungsi utama seperti issueCertificate untuk penerbitan, verifyCertificate untuk verifikasi, dan revokeCertificate untuk pencabutan sertifikat. Struktur kode *smart contract* akan dirancang secara modular untuk memastikan efisiensi dan keamanan operasional.

b) Pengujian Smart Contract Pengujian *smart contract* adalah tahapan vital untuk memastikan fungsionalitas dan keandalannya. Pengujian ini dilakukan menggunakan *framework* pengujian khusus seperti Hardhat atau Truffle. Proses pengujian mencakup verifikasi fungsionalitas dasar seperti kemampuan penerbitan, verifikasi, dan pencabutan sertifikat, serta memastikan bahwa semua kondisi dan *rule* dalam kontrak terpenuhi sesuai harapan.

c) Deployment Smart Contract Setelah melalui tahap penulisan dan pengujian yang ketat, *smart contract* akan di-*deploy* ke jaringan Polygon Mumbai Testnet. Proses *deployment* ini akan memanfaatkan *tools* seperti Hardhat. Setelah *deployment* berhasil, alamat *smart contract* yang unik akan diperoleh, dan alamat ini kemudian akan digunakan sebagai jembatan untuk integrasi dengan *frontend* (antarmuka pengguna) dan *backend* sistem, memungkinkan seluruh komponen berkomunikasi dan berfungsi secara harmonis.

3.5.2 Pengembangan Frontend

Antarmuka pengguna merupakan wajah dari sistem, krusial dalam menjembatani kompleksitas teknologi *blockchain* dengan kebutuhan interaksi harian pengguna. Pengembangan *frontend* ini difokuskan pada penciptaan pengalaman yang intuitif, responsif, dan lancar, memungkinkan pengguna untuk secara mudah menerbitkan, memverifikasi, dan mengelola sertifikat digital dalam lingkungan yang terdesentralisasi. Bagian ini menjadi kunci utama dalam memastikan bahwa kapabilitas sistem dapat diakses dan dimanfaatkan sepenuhnya oleh setiap pengguna, mengubah abstraksi teknis menjadi sebuah platform yang *user-friendly* dan efektif.

Aspek-aspek pengembangan *frontend* meliputi:

a) Setup Proyek Inisiasi proyek React.js dilakukan, diikuti dengan penambahan *library* esensial seperti Ethers.js. Komponen-komponen ini vital untuk membangun dasar aplikasi dan memfasilitasi interaksi dengan *blockchain* Polygon.
b) Integrasi dengan Smart Contract Koneksi antara aplikasi *frontend* dan *smart contract* yang sudah di-*deploy* di jaringan Polygon dibangun. Integrasi ini memungkinkan aplikasi untuk memanggil fungsi-fungsi *smart contract* utama seperti issueCertificate, verifyCertificate, dan revokeCertificate, serta membaca data *on-chain*.
c) Pembuatan Halaman Beberapa halaman inti didesain untuk mendukung fungsionalitas sistem. Ini termasuk Halaman Penerbitan Sertifikat untuk memasukkan data dan memicu proses penerbitan, Halaman Verifikasi Sertifikat yang memudahkan pemeriksaan keaslian, serta Halaman Riwayat Sertifikat untuk menampilkan daftar catatan historis yang komprehensif.
d) Integrasi dengan MetaMask *Wallet* MetaMask diintegrasikan sebagai alat utama untuk autentikasi pengguna dan penandatanganan transaksi. Integrasi ini memastikan pengguna

dapat berinteraksi secara aman dengan *smart contract* di Polygon, mengelola persetujuan transaksi, dan menangani *gas fee*.

e) Integrasi dengan Sistem Backend Untuk mendukung fungsionalitas tambahan yang memerlukan penyimpanan atau pemrosesan data di luar *blockchain*, *frontend* juga diintegrasikan dengan sistem *backend*. Integrasi ini memungkinkan *frontend* untuk mengambil atau mengirim data ke server terpusat saat operasi tertentu tidak memerlukan interaksi langsung dengan *smart contract*, seperti pengelolaan profil pengguna atau data non-esensial yang tidak memerlukan imutabilitas *blockchain*.

3.5.3 Pengembangan Backend

Pengembangan *backend* dilakukan untuk mendukung fungsi-fungsi tambahan yang tidak dapat diimplementasikan secara langsung oleh *smart contract* di *blockchain*, seperti penyimpanan dokumen sertifikat yang berukuran lebih besar dan pengelolaan data *off-chain* lainnya. Bagian *backend* ini berperan krusial dalam memastikan kelengkapan fungsionalitas sistem, khususnya untuk operasi yang memerlukan komputasi kompleks atau penyimpanan data dalam skala besar yang tidak efisien jika dilakukan langsung di *blockchain*. Proses pengembangan ini melibatkan beberapa langkah utama:

a) Setup Proyek Inisiasi proyek *backend* dilakukan menggunakan Node.js sebagai *runtime environment* dan Express.js sebagai *framework* untuk membangun API *server*. Selanjutnya, dependensi yang diperlukan akan ditambahkan, termasuk *library* seperti ipfs-http-client yang esensial untuk memfasilitasi interaksi dan integrasi dengan *InterPlanetary File System* (IPFS).

b) Pengelolaan Dokumen Sertifikat dan Integrasi IPFS *Backend* dikembangkan untuk memiliki kapabilitas dalam memproses dan mengelola dokumen sertifikat. Ini mencakup pembuatan fungsi untuk mengolah data sertifikat yang dikirimkan dari *frontend*, seperti mengubahnya menjadi format yang sesuai atau menambahkan metadata tertentu. Setelah persiapan data, *backend* akan bertanggung jawab untuk mengunggah dokumen sertifikat ini ke IPFS menggunakan *library* ipfs-http-client, yang kemudian akan mengembalikan *hash* unik sebagai referensi penyimpanan terdesentralisasi.

c) Implementasi API Endpoint Untuk memfasilitasi komunikasi antara *frontend* dan *backend*, berbagai API *endpoint* akan dibuat. Salah satu *endpoint* utamanya adalah untuk menangani

proses pengunggahan dokumen ke IPFS. *Endpoint* ini akan menerima data sertifikat dari *frontend*, memicu fungsi pengelolaan dokumen dan pengunggahan ke IPFS, lalu mengembalikan *hash* IPFS tersebut ke *frontend*. Hal ini memungkinkan *frontend* untuk kemudian mencatat *hash* IPFS ini ke dalam *smart contract* di *blockchain*, sehingga sertifikat digital tetap terhubung dengan dokumen aslinya yang tersimpan secara terdesentralisasi.

3.6 Pengujian Sistem

Validasi sistem merupakan tahapan fundamental dalam siklus pengembangan perangkat lunak, dilaksanakan untuk mengonfirmasi bahwa seluruh komponen yang telah dibangun beroperasi secara optimal, aman, dan efisien. Proses ini ditujukan untuk memverifikasi bahwa sistem tidak hanya memenuhi spesifikasi fungsional yang telah dirancang, tetapi juga menunjukkan kinerja yang memadai serta ketahanan terhadap potensi kerentanan. Secara spesifik, pengujian ini mencakup evaluasi mendalam terhadap aspek fungsionalitas, keamanan, dan kinerja sistem secara komprehensif.

3.6.1 Pengujian Fugsionalitas

Pengujian fungsionalitas dirancang untuk memverifikasi kesesuaian operasi semua fitur sistem dengan persyaratan yang telah ditetapkan. Tahap ini berkonsentrasi pada validasi setiap kapabilitas inti dari sistem penerbitan dan verifikasi sertifikat digital.

a) Penerbitan Sertifikat Pengujian ini memastikan bahwa penerbit dapat berhasil menerbitkan sertifikat dengan memasukkan data yang diperlukan, serta memverifikasi bahwa data sertifikat yang diterbitkan tersimpan dengan benar di *blockchain* Polygon.
b) Verifikasi Sertifikat Tahap ini memverifikasi bahwa penerima sertifikat atau pihak ketiga dapat memverifikasi keaslian sertifikat dengan mudah, baik melalui *file* sertifikat maupun *hash* sertifikat, dan memastikan bahwa hasil verifikasi yang ditampilkan sesuai dengan status sertifikat yang tersimpan di *blockchain*.
c) Pencabutan Sertifikat Pengujian dilakukan untuk memastikan bahwa penerbit yang berwenang dapat mencabut sertifikat yang telah diterbitkan, dan bahwa status sertifikat tersebut secara akurat berubah menjadi tidak valid setelah proses pencabutan berhasil dicatat di *blockchain*.

3.6.2 Pengujian Kinerja

Pengujian kinerja bertujuan untuk mengevaluasi kemampuan sistem dalam beroperasi dengan kecepatan dan efisiensi yang optimal di bawah beragam beban kerja. Pengujian ini juga mengukur efektivitas pemanfaatan sumber daya sistem. Penilaian ini krusial untuk menentukan skalabilitas dan kelayakan implementasi sistem dalam kondisi penggunaan nyata pada jaringan Polygon.

a) Kecepatan Transaksi Pengujian ini melibatkan pengukuran waktu yang dibutuhkan untuk menyelesaikan berbagai operasi kunci, seperti menerbitkan, memverifikasi, dan mencabut sertifikat. Hasil pengukuran akan dianalisis untuk mengevaluasi respons sistem.
b) Biaya Gas Fee Pengujian akan mengukur secara akurat biaya *gas fee* yang dikeluarkan untuk setiap jenis transaksi yang dilakukan di jaringan Polygon, seperti penerbitan dan verifikasi sertifikat. Analisis biaya ini penting untuk menilai efisiensi operasional sistem.
c) Skalabilitas Pengujian skalabilitas dilakukan untuk mengevaluasi kemampuan sistem dalam menangani volume transaksi yang besar. Hal ini meliputi pengujian penerbitan atau verifikasi sejumlah besar sertifikat secara bersamaan, sambil mengukur waktu dan biaya *gas fee* yang dibutuhkan untuk memverifikasi bahwa sistem dapat berkinerja stabil di bawah beban tinggi.

BAB 4 HASIL DAN PEMBAHASAN

4.1 Gambaran Umum Implementasi Sistem

Pengantar singkat mengenai hasil dari tahap pengembangan sistem. * Penjelasan mengenai *environment* pengembangan dan *deployment* yang digunakan. * Arsitektur sistem secara keseluruhan dalam konteks hasil implementasi.

4.2 Hasil Implementasi Sistem

* Bagian ini akan menampilkan wujud fisik dari sistem yang telah dikembangkan. * **4.2.1 Implementasi Smart Contract** * Deskripsi singkat mengenai *smart contract* yang berhasil di-*deploy* di jaringan Polygon. * Tampilan *Contract Address* di Polygonscan (opsional, jika ingin menampilkan bukti *deployment*). * Penjelasan fungsi-fungsi utama yang terimplementasi (issueCertificate, verifyCertificate, revokeCertificate). * **4.2.2 Implementasi Frontend (Antarmuka Pengguna)** * Tampilan *(screenshot)* Halaman Penerbitan Sertifikat, dengan penjelasan mengenai fitur-fitur yang ada. * Tampilan *(screenshot)* Halaman Verifikasi Sertifikat, dengan penjelasan mengenai cara verifikasi. * Tampilan *(screenshot)* Halaman Riwayat Sertifikat, dengan penjelasan mengenai informasi yang ditampilkan. * Penjelasan mengenai integrasi *wallet* (MetaMask) dan bagaimana pengguna berinteraksi. * **4.2.3 Implementasi Backend (Opsional/Jika Ada)** * Penjelasan mengenai *endpoint* API yang telah dibuat. * Cara *backend* terintegrasi dengan IPFS untuk penyimpanan dokumen.

4.3 Hasil Pengujian Sistem

* Bagian ini akan menyajikan data dan temuan dari pengujian yang telah dilakukan. * **4.3.1 Hasil Pengujian Fungsionalitas** * Penyajian hasil pengujian setiap fungsi (Penerbitan, Verifikasi, Pencabutan Sertifikat). * Tabel atau narasi yang menunjukkan status pengujian (berhasil/gagal) dan deskripsi singkat. * Pembuktian bahwa sistem bekerja sesuai dengan persyaratan fungsional. * **4.3.2 Hasil Pengujian Kinerja** * **4.3.2.1 Kecepatan Transaksi:** * Penyajian data pengukuran waktu rata-rata untuk setiap jenis transaksi (penerbitan, verifikasi, pencabutan). * Gunakan grafik atau tabel untuk visualisasi data jika diperlukan. * Analisis singkat terhadap hasil yang diperoleh. * **4.3.2.2 Biaya Gas Fee:** * Penyajian data pengukuran biaya *gas fee* rata-rata untuk setiap jenis transaksi di jaringan Polygon. * Gunakan grafik atau tabel untuk visualisasi data (misalnya perbandingan Gwei vs. USD). * Analisis singkat terhadap biaya yang dikeluarkan dan efisiensinya. * **4.3.2.3 Skalabilitas:** * Penyajian hasil pengujian skalabilitas (misalnya waktu dan biaya untuk sejumlah besar transaksi). * Analisis performa sistem saat menangani beban tinggi.

4.4 Pembahasan

* Bagian ini adalah inti dari analisis Anda, di mana Anda menginterpretasikan hasil dan menghubungkannya dengan teori serta tujuan penelitian. * **4.4.1 Analisis Hasil Implementasi dan Kinerja** * Interpretasi mendalam terhadap hasil implementasi dan pengujian kinerja. * Bagaimana *smart contract* Polygon berhasil mengatasi masalah *gas fee* dan kecepatan yang disebutkan di Bab 1. * Pembahasan mengenai keunggulan sistem yang terdesentralisasi dan aman dalam penerbitan/verifikasi sertifikat. * Bagaimana sistem mendukung model SaaS (banyak penerbit). * **4.4.2 Hubungan dengan Rumusan Masalah** * Jawab setiap rumusan masalah yang telah Anda ajukan di Bab 1 secara terperinci, berdasarkan hasil yang telah disajikan. * Pastikan setiap pertanyaan penelitian memiliki jawaban yang kuat dan didukung

oleh data. * **4.4.3 Perbandingan dengan Penelitian Terkait** * Diskusikan persamaan dan perbedaan sistem Anda dengan penelitian terdahulu yang Anda cantumkan di Bab 2. * Soroti kontribusi unik atau peningkatan yang dibawa oleh penelitian Anda. * **4.4.4 Tantangan dan Solusi (Opsional)** * Identifikasi tantangan yang dihadapi selama pengembangan atau pengujian, dan bagaimana Anda mengatasinya. * **4.4.5 Implikasi Penelitian** * Diskusikan implikasi praktis dan teoretis dari temuan Anda. * Bagaimana hasil penelitian ini dapat bermanfaat bagi industri atau bidang terkait.

BAB 5HASIL DAN PEMBAHASAN

DAFTAR PUSTAKA

[1] K. Badan Pengembangan dan Pembinaan Bahasa, “Sertifikat.” Accessed: Jan. 27, 2025. [Online]. Available: https://kbbi.kemdikbud.go.id/entri/sertifikat

[2] S. A. Habibi, G. S. Prambudi, T. Trisnawati, and R. Wulandari, “Transformasi Digital Administrasi Pertanahan : Implementasi Dan Tantangan Sertipikat Elektronik Di Indonesia,” 2025.

[3] S. Hidayah, “Tantangan dan Peluang Sertifikat Elektronik dalam Reformasi Pendaftaran Tanah di Era Digital .,” vol. 1, no. 6, pp. 186–199, 2024.

[4] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, “Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing,” *Future Internet*, vol. 14, no. 11, pp. 1–22, 2022, doi: 10.3390/fi14110341.

[5] Y. Hu and S. Peng, “A Decentralized Voting System on the Polygon Blockchain,” *Procedia Comput Sci*, vol. 247, no. C, pp. 1304–1313, 2023, doi: 10.1016/j.procs.2024.10.156.

[6] K. C. Maharana and S. Acharya, “International Journal of Research Publication and Reviews,” *SSRN Electronic Journal*, no. 5, pp. 9654–9660, 2024, doi: 10.2139/ssrn.4909110.

[7] H. Khandelwal, K. Mittal, S. Agrawal, and H. Jain, “Certificate verification system using blockchain,” *Lecture Notes in Electrical Engineering*, vol. 643, no. January, pp. 251–257, 2020, doi: 10.1007/978-981-15-3125-5_27.

[8] H. Khandelwal, K. Mittal, S. Agrawal, and H. Jain, “Certificate verification system using blockchain,” *Lecture Notes in Electrical Engineering*, vol. 643, no. January, pp. 251–257, 2020, doi: 10.1007/978-981-15-3125-5_27.

[9] W. Swastika, H. Wirasantosa, and O. H. Kelana, “Rancang Bangun Website Akademik dengan Penyimpanan Sertifikat Digital Menggunakan Teknologi Blockchain,” *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 1, p. 33, 2022, doi: 10.25126/jtiik.2021863645.

[10] W. Swastika, H. Wirasantosa, and O. H. Kelana, “Rancang Bangun Website Akademik dengan Penyimpanan Sertifikat Digital Menggunakan Teknologi Blockchain,” *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 1, p. 33, 2022, doi: 10.25126/jtiik.2021863645.

[11] S. Oknora Firza, Yuhandri, and Sumijan, “Teknologi Blockchain dalam Keamanan Sertifikat Menggunakan Smart Contracts dan Distributed Ledger pada Platfrom Edutech,” *KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)*, vol. 5, no. 2, pp. 587–594, 2024.

[12] “mrizal1,+312.+Jurnal+Rusydi+JRPP+S5+Pendidikan”.

[13] E. W. Fridayanthie, H. Haryanto, and T. Tsabitah, “Penerapan Metode Prototype Pada Perancangan Sistem Informasi Penggajian Karyawan (Persis Gawan) Berbasis Web,” *Paradigma - Jurnal Komputer dan Informatika*, vol. 23, no. 2, Sep. 2021, doi: 10.31294/p.v23i2.10998.