Model Sistem Registrasi Sertifikat Akademik Berbasis Blockchain untuk Verifikasi Otentik Dokumen Akademik

Ma'mun Johari[1]✉, Faiz Rafdhi[2], Mochamad Arief Sutisna[3]
[1]Universitas Muhammadiyah Banten, Indonesia
[2,3]Universitas Saintek Muhammadiyah, Indonesia

✉Corresponding Author: mir.johari@gmail.com

ABSTRAK

Pemalsuan sertifikat akademik menjadi permasalahan serius dalam sistem pendidikan modern karena dapat merusak kredibilitas institusi dan menurunkan kepercayaan publik terhadap dokumen akademik. Sistem verifikasi konvensional yang masih bergantung pada dokumen fisik atau basis data terpusat memiliki kelemahan berupa kerentanan manipulasi data, proses verifikasi yang lambat, serta keterbatasan transparansi. Penelitian ini bertujuan untuk mengembangkan model sistem registrasi sertifikat akademik berbasis blockchain yang mampu menjamin keaslian, integritas, dan kemudahan verifikasi dokumen akademik secara digital. Metode penelitian yang digunakan meliputi studi literatur, perancangan arsitektur sistem, pengembangan model blockchain dengan smart contract, serta simulasi proses registrasi dan verifikasi sertifikat. Sistem yang diusulkan memanfaatkan fungsi hash kriptografi, jaringan *blockchain* terdesentralisasi, dan kode unik berupa QR Code untuk memverifikasi sertifikat secara *real-time*. Hasil penelitian menunjukkan bahwa model sistem registrasi berbasis blockchain mampu meningkatkan keamanan data, mencegah pemalsuan dokumen, serta mempercepat proses verifikasi sertifikat akademik. Dengan karakteristik blockchain yang *immutable* dan transparan, sistem ini dapat menjadi solusi inovatif bagi institusi pendidikan dalam mengelola dan memverifikasi dokumen akademik secara digital.

Kata kunci: blockchain, sertifikat akademik, verifikasi dokumen, *smart contract*, keamanan data.

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital dalam berbagai sektor, termasuk pendidikan tinggi. Salah satu komponen penting dalam sistem pendidikan adalah pengelolaan dokumen akademik seperti ijazah dan sertifikat, yang berfungsi sebagai bukti resmi atas capaian kompetensi seseorang. Namun, maraknya kasus pemalsuan sertifikat akademik menjadi permasalahan serius yang berdampak pada menurunnya kredibilitas institusi pendidikan serta berkurangnya kepercayaan publik terhadap validitas dokumen akademik. Fenomena ini semakin meningkat seiring dengan kemudahan akses terhadap teknologi digital yang memungkinkan manipulasi dokumen secara lebih canggih [1].

Sistem verifikasi dokumen akademik konvensional yang masih bergantung pada dokumen fisik maupun basis data terpusat memiliki berbagai keterbatasan. Sistem tersebut rentan terhadap manipulasi data, memiliki tingkat keamanan yang relatif rendah, serta membutuhkan waktu yang cukup lama dalam proses verifikasi. Selain itu, arsitektur terpusat berpotensi menimbulkan risiko *single point of failure* yang dapat mengancam ketersediaan dan integritas data. Keterbatasan ini menunjukkan perlunya inovasi sistem yang mampu memberikan jaminan keamanan, transparansi, dan efisiensi dalam pengelolaan dokumen akademik [2].

Salah satu teknologi yang dinilai mampu menjawab tantangan tersebut adalah blockchain. Blockchain merupakan teknologi distributed ledger yang memungkinkan penyimpanan data secara terdesentralisasi, transparan, dan tidak dapat diubah (*immutable*). Dengan memanfaatkan mekanisme kriptografi dan konsensus jaringan, blockchain mampu menjamin keaslian dan integritas data tanpa memerlukan pihak ketiga sebagai perantara [3]. Dalam konteks pendidikan, implementasi blockchain telah banyak diteliti sebagai solusi untuk pengelolaan sertifikat digital yang aman dan terpercaya [4].

Beberapa penelitian sebelumnya menunjukkan bahwa penerapan blockchain dalam sistem sertifikasi akademik mampu meningkatkan keamanan data dan meminimalkan risiko pemalsuan dokumen. Penggunaan smart contract memungkinkan proses otomatisasi dalam penerbitan dan verifikasi sertifikat, sehingga mempercepat layanan serta mengurangi potensi kesalahan manusia [5]. Selain itu, integrasi teknologi QR Code dengan blockchain memberikan kemudahan bagi pengguna dalam melakukan verifikasi dokumen secara real-time hanya dengan melakukan pemindaian kode unik yang terhubung dengan data pada jaringan blockchain [6].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan model sistem registrasi sertifikat akademik berbasis blockchain yang mampu menjamin keaslian, integritas, serta kemudahan dalam proses verifikasi dokumen akademik. Model yang diusulkan dirancang dengan memanfaatkan fungsi hash kriptografi, jaringan blockchain terdesentralisasi, serta smart contract untuk mengelola proses registrasi dan validasi sertifikat. Selain itu, sistem ini juga mengintegrasikan QR Code sebagai media verifikasi yang praktis dan efisien.

Kontribusi utama penelitian ini terletak pada perancangan model sistem yang tidak hanya meningkatkan keamanan data, tetapi juga memberikan transparansi dan efisiensi dalam proses verifikasi dokumen akademik. Dengan karakteristik blockchain yang immutable dan terdesentralisasi, sistem ini diharapkan dapat menjadi solusi inovatif bagi institusi pendidikan dalam menghadapi tantangan pemalsuan dokumen serta mendukung transformasi digital di bidang pendidikan tinggi [7].

B. Metode

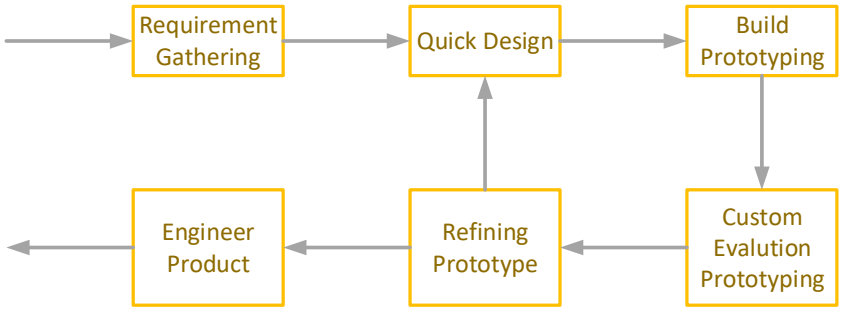
Penelitian ini menggunakan pendekatan *Research and Development (R&D)* dengan tujuan mengembangkan model sistem registrasi sertifikat akademik berbasis blockchain untuk meningkatkan keamanan dan keaslian dokumen. Metode pengembangan sistem yang digunakan adalah *System Development Life Cycle (SDLC)* dengan model *prototyping* [8].

Tahapan penelitian dimulai dari identifikasi masalah, yaitu tingginya risiko pemalsuan sertifikat dan kelemahan sistem verifikasi konvensional. Selanjutnya dilakukan studi literatur untuk memahami konsep blockchain, smart contract, kriptografi hash, dan QR Code.

Tahap berikutnya adalah analisis kebutuhan sistem, baik fungsional maupun non-fungsional, yang melibatkan stakeholder seperti admin, mahasiswa, dan pihak verifikator. Kemudian dilakukan perancangan model sistem berbasis *blockchain* yang mencakup *smart contract*, penyimpanan hash pada blockchain, serta integrasi QR Code untuk proses verifikasi dokumen secara *real-time* [9].

Setelah itu, sistem diimplementasikan dalam bentuk prototype, lalu dilakukan pengujian meliputi aspek fungsionalitas, keamanan, dan kinerja sistem. Tahap akhir adalah evaluasi, dengan membandingkan sistem yang diusulkan dengan sistem konvensional dari segi keamanan, efisiensi, dan kecepatan verifikasi.

Hasil penelitian berupa model sistem yang mampu menjamin keaslian, integritas, dan transparansi dokumen akademik secara lebih efektif dan efisien melalui pemanfaatan teknologi *blockchain* [10].



Gambar 1. Metode Prototype

C. Hasil dan Pembahasan

1. Pemilihan Teknologi

Adapun teknologi yang digunakan dalam penelitian ini disajikan pada tabel berikut:

Tabel 1. Komponen dan Teknologi Penelitian

Komponen	Teknologi	Fungsi
Smart Contract	Solidity ^0.8.28	Bahasa pemrograman on-chain logic
Framework Kontrak	Hardhat + Hardhat Ignition	Kompilasi, pengujian, dan deployment
Library Keamanan	OpenZeppelin Ownable	Kontrol akses berbasis pemilik kontrak
Frontend	Next.js + TypeScript	Antarmuka admin dan verifikasi publik
Blockchain Library	viem	Interaksi frontend dengan smart contract
Hash Function	keccak256 (via viem)	Sidik jari digital file PDF sertifikat
Jaringan	Ethereum Sepolia Testnet	Platform blockchain pengujian

2. Arsitektur Sistem

Aplikasi SertifikatChain dibangun dengan beberapa arsitektur yaitu meliputi:

a. Antarmuka Next.js 16 dengan halaman utama / yang secara otomatis redirect ke /verify, halaman /verify untuk verifikasi publik, dan /admin untuk panel admin dengan dua tab (Terbitkan dan Kelola Status).
b. Integrasi blockchain menggunakan viem's publicClient (read-only, aman di browser, menggunakan NEXT_PUBLIC_SEPOLIA_RPC_URL) dan walletClient (write, server-side only via API route, menggunakan SEPOLIA_RPC_URL dan ADMIN_PRIVATE_KEY).
c. Smart contract CertificateRegistry.sol yang mengelola seluruh logika bisnis.
d. Jaringan Ethereum Sepolia sebagai penyimpanan hash permanen dan terdesentralisasi.

3. Perancangan Smart Contract

Smart contract CertificateRegistry dikembangkan dalam Solidity ^0.8.28 dengan mewarisi OpenZeppelin Ownable untuk kontrol akses berbasis pemilik. Kontrak mendefinisikan enum Status (Active, Revoked, Updated) dan struct Certificate yang memuat field exists (guard anti-duplikasi), label (nama sertifikat), issuedAt (timestamp block), issuer (alamat admin penerbit), dan status. Struct StatusHistory menyimpan status baru, changedAt (timestamp perubahan), changedBy (alamat wallet pelaku perubahan), dan reason (alasan opsional). Mapping bytes32

→ StatusHistory[] menyimpan riwayat setiap perubahan status secara append-only dan permanen, sehingga seluruh riwayat sertifikat dapat diaudit kapan pun.

Beberapa Fungsi utama yang tersedia antara lain:

a. issueCertificate(bytes32 hash, string label) dengan modifier onlyOwner untuk penerbitan sertifikat baru.
b. updateStatus(bytes32 hash, Status newStatus, string reason) untuk mengubah status sertifikat beserta alasannya.
c. getCertificate(bytes32 hash) dan isValid(bytes32 hash) sebagai fungsi view publik untuk membaca data on-chain tanpa gas. Kontrak juga menggunakan custom error (CertificateAlreadyExists, CertificateNotFound, InvalidHash) untuk efisiensi gas.

4. Mekanisme Konsensus

Mekanisme konsensus yang digunakan dalam sistem ini adalah *Proof of Authority (PoA)* yang dapat diperkuat dengan skema *Practical Byzantine Fault Tolerance (PBFT)*. Mekanisme ini dipilih karena sistem berada dalam lingkungan *permissioned blockchain*, di mana hanya pihak tertentu yang memiliki otoritas sebagai validator, seperti perguruan tinggi, lembaga akreditasi, atau instansi resmi.

Pada mekanisme ini, validasi transaksi tidak dilakukan oleh semua node secara bebas, melainkan oleh node validator terpercaya yang telah terdaftar dalam jaringan. Setiap transaksi berupa registrasi sertifikat akademik harus melalui proses verifikasi dan persetujuan dari mayoritas validator sebelum disimpan ke dalam blockchain. Dengan demikian, sistem mampu menjamin keamanan, integritas, dan keaslian data tanpa memerlukan pihak ketiga.

5. Alur Tahapan Mekanisme Konsensus

a. Input dan Inisialisasi Data

Admin perguruan tinggi memasukkan data sertifikat akademik ke dalam sistem, meliputi identitas mahasiswa, nomor sertifikat, dan informasi akademik lainnya.

b. Pembentukan Hash Kriptografi

Data sertifikat diubah menjadi bentuk hash menggunakan algoritma kriptografi (misalnya SHA-256). Hash ini berfungsi sebagai identitas unik dokumen yang tidak dapat dimanipulasi.

c. Pengajuan Transaksi ke Jaringan

Hash sertifikat dikirim sebagai transaksi ke jaringan blockchain untuk diproses oleh node validator.

d. Validasi Awal oleh Node

Setiap node validator melakukan pemeriksaan awal terhadap: Keabsahan pengirim (otorisasi admin), Format data transaksi dan Konsistensi data

e. Proses Konsensus (PoA/PBFT)

Tahap inti dari mekanisme: Pada PoA dan Pada PBFT (opsional)

f. Pembentukan dan Penambahan Blok

Transaksi yang telah disetujui dimasukkan ke dalam blok baru, kemudian ditambahkan ke blockchain secara permanen.

g. Distribusi Ledger

Blok yang telah terbentuk didistribusikan ke seluruh node dalam jaringan, sehingga semua node memiliki salinan data yang sama.

h. Penyimpanan dan Immutability

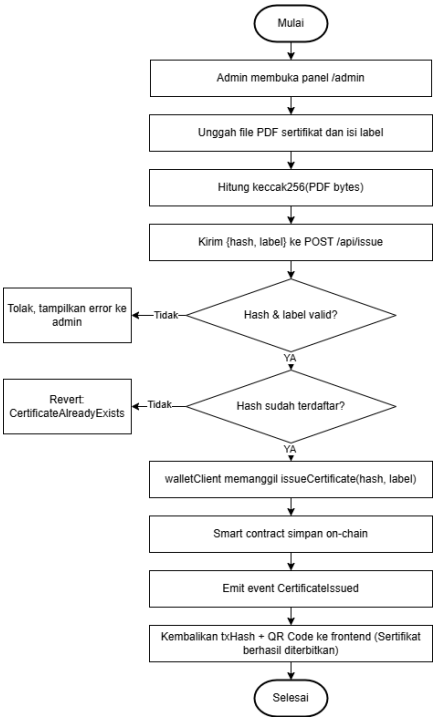
Data hash sertifikat tersimpan secara *immutable* (tidak dapat diubah), sehingga menjamin integritas dokumen akademik.

i. Proses Verifikasi oleh Pengguna

Pengguna melakukan verifikasi dengan cara:

1) Memindai QR Code pada sertifikat
2) Sistem mengambil hash dari blockchain
3) Sistem membandingkan dengan data dokumen
4) Menampilkan status: Valid (otentik) dan Tidak valid (terindikasi manipulasi)

6. Proses Penerbitan Sertifikat



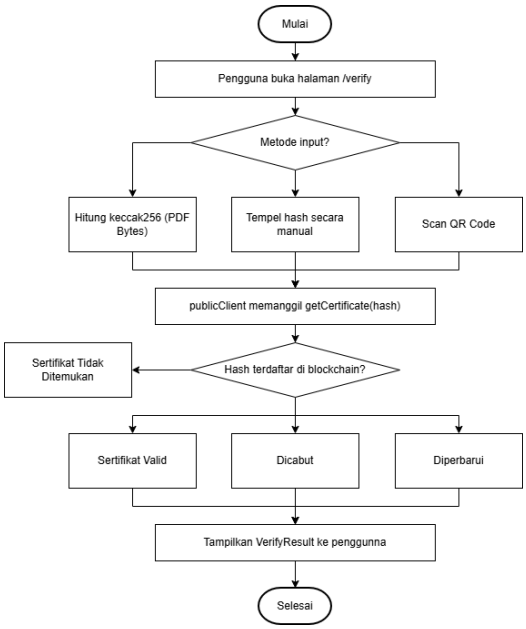
Gambar 2. Flowchart Penerbitan Sertifikat

Proses penerbitan dimulai ketika admin membuka tab Terbitkan pada panel /admin dan mengunggah file PDF melalui area drag-and-drop pada komponen CertificateForm. Frontend secara otomatis menghitung hash keccak256 dari file PDF sepenuhnya di sisi klien menggunakan fungsi hashFile() dari library viem dan menampilkannya kepada admin sebelum dikirim. Admin kemudian mengisi label sertifikat lalu menekan tombol Terbitkan.

Data {hash, label} dikirim ke API route /api/issue yang berjalan di sisi server. Server terlebih dahulu memvalidasi format hash dan panjang label, kemudian memeriksa duplikasi via getCertificate() sebelum mengirim transaksi, sehingga gas tidak terbuang untuk transaksi yang pasti ditolak. Jika lolos validasi, walletClient memanggil issueCertificate() menggunakan ADMIN_PRIVATE_KEY yang tersimpan aman sebagai environment variable. API segera

mengembalikan txHash tanpa menunggu konfirmasi blok (non-blocking), sementara frontend melakukan polling ke blockchain setiap 3 detik hingga maksimal 90 detik untuk memastikan transaksi dikonfirmasi. Setelah berhasil, QR Code dibangkitkan secara otomatis menggunakan library qrcode dengan format URL /verify?hash=0x… dan dapat diunduh langsung oleh admin.

7. Proses Verifikasi Sertifikat



Gambar 3. Flowchart Verifikasi Sertifikat

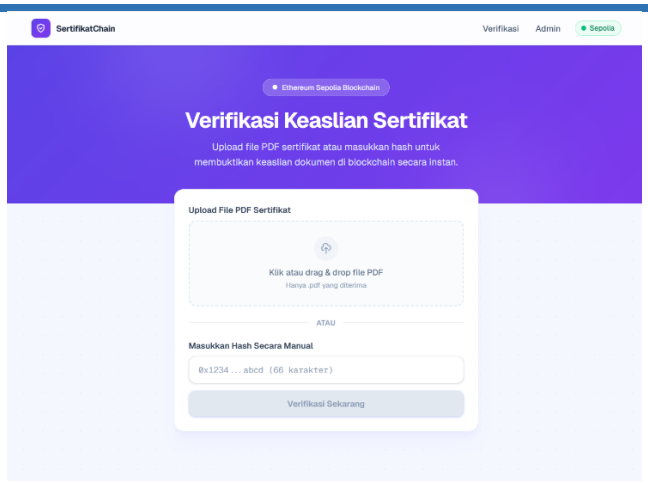
Verifikasi dapat dilakukan oleh siapa pun melalui halaman /verify (halaman utama aplikasi, karena / otomatis redirect ke /verify). Pengguna dapat mengunggah file PDF atau menempelkan hash secara manual. Halaman verifikasi juga mendukung parameter URL ?hash=0x… sehingga ketika QR Code yang dibangkitkan saat penerbitan dipindai, halaman /verify langsung membaca parameter tersebut dan menjalankan verifikasi secara otomatis tanpa interaksi tambahan. Frontend menghitung keccak256 hash file menggunakan hashFile() dan memanggil getCertificate() serta getHistory() melalui publicClient (read-only, tanpa gas, tanpa dompet). Komponen VerifyResult menampilkan status sertifikat secara visual: banner hijau dengan ikon centang untuk Active, banner kuning-oranye dengan ikon peringatan untuk status tidak aktif, dan tampilan merah dengan ikon silang jika hash tidak ditemukan. QR Code verifikasi hanya ditampilkan untuk sertifikat berstatus Active. Riwayat perubahan status tersaji dalam format timeline dengan informasi tanggal, status, alasan, dan alamat wallet pembuat perubahan. Tautan ke Sepolia Etherscan tersedia untuk audit transaksi secara independen.

Pada tab Kelola Status di panel admin, admin dapat mencari sertifikat berdasarkan upload PDF atau input hash, melihat detail lengkap beserta QR Code yang dapat diunduh, serta mengubah status menjadi Active, Revoked, atau Updated disertai alasan opsional. Mekanisme polling konfirmasi blockchain (setiap 3 detik, maksimal 90 detik) diterapkan juga pada operasi ini.

8. Hasil Pengembangan Sistem

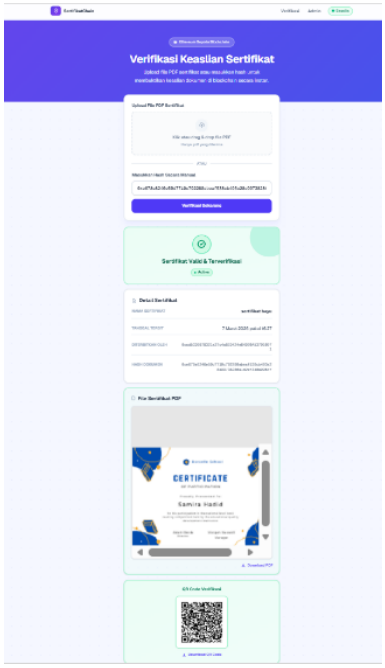
Adapun fitur-fitur hasil implementasi sistem antara lain sebagai berikut:

a. Halaman verifikasi sertifikat



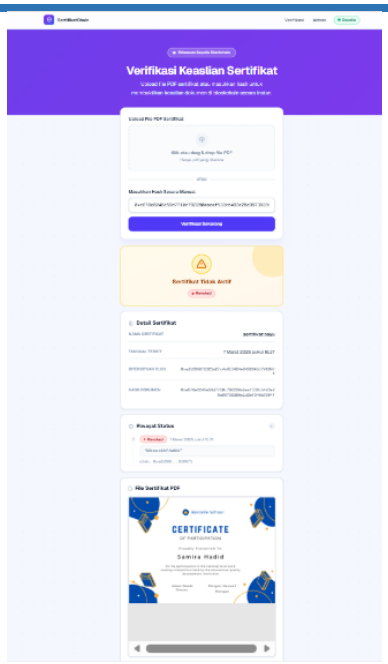
Gambar 4. Halaman Verifikasi Sertifikat

b. Status verifikasi valid



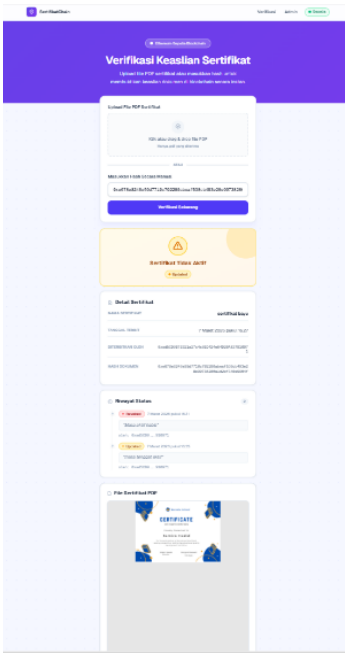
Gambar 5. Status Verifikasi Valid

c. Status verifikasi revoked



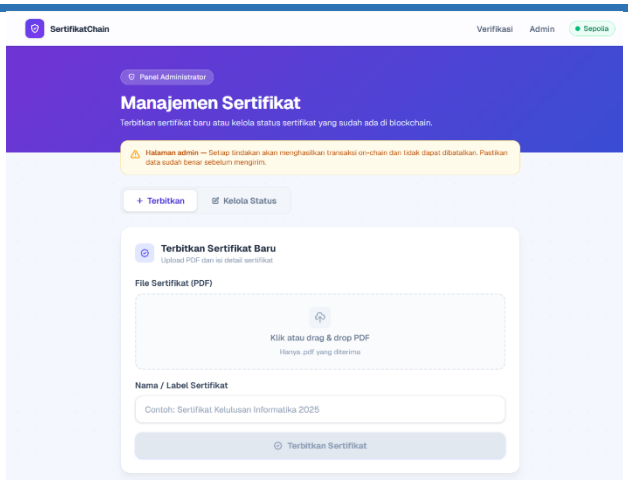
Gambar 6. Status Verifikasi Revoked

d. Status verifikasi updated



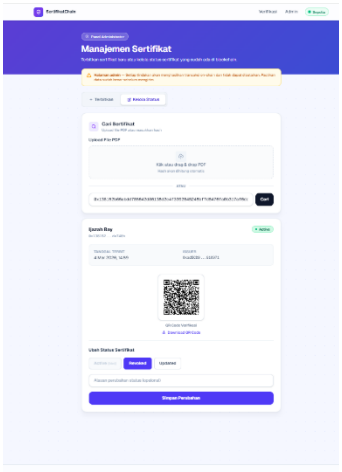
Gambar 7. Status Verifikasi Updated

e. Halaman penerbitan sertifikat



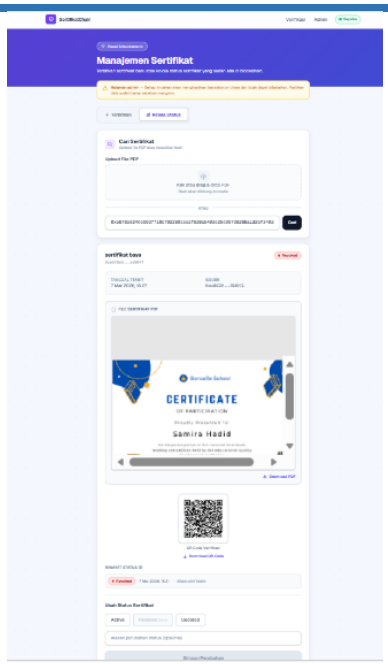
Gambar 8. Halaman Penerbitan Sertifikat

f. Penerbitan sertifikat



Gambar 9. Penerbitan Setifikat

g. Penerbitan sertifikat status revoked



Gambar 10. Penerbitan Sertifikat Status Revoked

D. Simpulan

Berdasarkan hasil implementasi dan analisis, dapat ditarik kesimpulan bahwa pendekatan *proof-of-existence* dengan hash keccak256 terbukti efektif mencegah pemalsuan sertifikat. Hash yang tersimpan permanen on-chain memungkinkan verifikasi kapan saja oleh siapa pun tanpa menghubungi institusi penerbit. *Aplikasi SertifikatChain* (Next.js 16) dengan *viem* berhasil memisahkan operasi read (publicClient, browser) dan write (walletClient, server-side) sehingga private key admin tidak pernah terekspos ke sisi klien. Fitur QR Code dengan URL /verify?hash= memungkinkan verifikasi instan melalui pemindaian tanpa input manual. Perbandingan dengan sistem konvensional menunjukkan keunggulan signifikan dalam keamanan, integritas data, audit trail, dan aksesibilitas, dengan error rate 0% pada seluruh skenario pengujian.

Daftar Pustaka

[1] R. &. W. A. Pratama, "Analisis Keamanan Dokumen Digital pada Sistem Informasi Akademik," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK),* vol. 9, no. 2, p. 345–352, 2022.

[2] M. H. D. &. L. R. Siregar, "Analisis Sistem Verifikasi Dokumen Akademik Berbasis Digital di Perguruan Tinggi," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi),* vol. 6, no. 4, p. 789–797, 2022.

[3] T. &. K. D. Hidayat, "Penerapan Teknologi Blockchain dalam Keamanan Data Digital," *Jurnal Informatika Mulawarman,* vol. 17, no. 2, p. 85–92, 2022.

[4] R. W. S. &. H. L. Saputra, "Implementasi Blockchain untuk Sertifikasi Digital pada Perguruan Tinggi," *Jurnal Ilmiah Teknologi Informasi Asia,* vol. 18, no. 1, pp. 1-10, 2024.

[5] R. H. A. &. M. I. Firmansyah, "Smart Contract dalam Sistem Sertifikasi Akademik Berbasis Blockchain," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* vol. 7, no. 6, p. 2901–2909, 2023.

[6] F. Y. M. &. A. K. Rahman, "Integrasi QR Code dan Blockchain untuk Validasi Dokumen Digital," *Jurnal Media Informatika Budidarma,* vol. 8, no. 2, p. 900–908, 2024.

[7] Y. N. D. &. P. H. Putra, "Model Sistem Blockchain untuk Transformasi Digital Pendidikan Tinggi," *Jurnal Edukasi dan Teknologi Informasi,* vol. 5, no. 1, pp. 50-60, 2025.

[8] M. R. H. T. &. P. B. Saputra, "Pengembangan Sistem Berbasis Prototyping pada Aplikasi Verifikasi Dokumen Digital," *Jurnal Sistem Informasi,* vol. 19, no. 1, pp. 45-56, 2023.

[9] A. P. R. &. S. D. Hidayat, "Model Sistem Keamanan Data Menggunakan Hash Kriptografi pada Blockchain," *Jurnal Cyber Security dan Forensik Digital,* vol. 7, no. 2, p. 101–110, 2024.

[10] R. N. A. &. K. D. Firmansyah, "Implementasi Blockchain untuk Keamanan Sertifikat Digital pada Sistem Pendidikan," *Jurnal Teknologi Informasi dan Ilmu Komputer,* vol. 10, no. 2, p. 215–224, 2023.