Pengembangan Decentralized Application (DApp) untuk Manajemen Sertifikat Digital menggunakan Non-Fungible Tokens (NFT) berbasis Standar ERC-721 di Jaringan Ethereum

Bayu Al Ikhlas Swari[1], I Made Suartana[2],

[1,3] Jurusan Teknik Informatika/Program Studi S1 Teknik Informatika, Universitas Negeri Surabaya
[1]bayual.20073@mhs.unesa.ac.id
[2]madesuartana@unesa.ac.id

***Abstrak*— Penelitian ini mengembangkan aplikasi terdesentralisasi (DApp) untuk manajemen sertifikat digital menggunakan Non-Fungible Token (NFT) berbasis standar ERC-721 di jaringan Ethereum. Aplikasi ini dirancang untuk meningkatkan keamanan, dan transparansi dalam pembuatan, pengelolaan, serta verifikasi sertifikat digital. Hasil penelitian menunjukan bahwa penggunaan teknologi blockchain memberikan jaminan bahwa setiap sertifikat yang diterbitkan tidak hanya dapat dilacak dan diverifikasi secara publik, tetapi juga tidak dapat diubah atau dimanipulasi setelah diterbitkan. Hal ini membuat sistem lebih aman dibandingkan dengan metode tradisional. Implementasi standar ERC-721 memungkinkan setiap sertifikat digital yang diterbitkan dalam bentuk NFT memiliki identitas unik yang tidak dapat diduplikasi atau dipalsukan. Selain itu, teknologi ini juga memungkinkan pemilik sertifikat untuk memiliki bukti kepemilikan yang aman dan dapat diverifikasi oleh pihak ketiga. Pengembangan dan pengujian smart contract yang ditulis dalam bahasa pemrograman Solidity pada platform Ethereum juga berhasil membuktikan bahwa smart contract yang dibuat berfungsi dengan baik dalam berbagai aspek seperti penciptaan, transfer, verifikasi, dan penghapusan sertifikat. Smart contract ini menunjukkan keamanan sesuai dengan spesifikasi yang diharapkan, menjadikannya solusi inovatif untuk manajemen sertifikat digital.**

Kata Kunci— **Blockchain, Ethereum, DApp, Sertifikat Digital, NFT, ERC-721.**

I. PENDAHULUAN

Kebutuhan akan sertifikat digital yang aman, transparan, dan mudah diverifikasi semakin meningkat dalam berbagai sektor, seperti pendidikan dan sertifikasi profesional. Namun, tantangan utama yang masih dihadapi adalah memastikan keaslian dan validitas sertifikat tersebut. Teknologi blockchain telah muncul sebagai solusi potensial untuk masalah ini. Secara konsep, blockchain adalah serangkaian blok yang saling terhubung dan menyimpan informasi dengan tanda tangan digital, menciptakan sistem yang terdesentralisasi, transparan, dan aman [1]. Salah satu implementasi blockchain yang menonjol adalah Non-Fungible Tokens (NFT), yang dapat mewakili aset digital unik dan berharga [2], termasuk sertifikat digital.

Ethereum, sebagai blockchain terbesar yang mengadopsi smart contract [3], menyediakan platform yang ideal untuk pengembangan aplikasi terdesentralisasi (DApps) dan implementasi NFT. Dengan standar ERC-721, token di Ethereum memungkinkan setiap sertifikat memiliki identitas unik yang tidak dapat dipalsukan, serta dapat diverifikasi secara publik melalui blockchain [4]. EIP-721, sebagai bagian dari ERC-721, menyediakan fungsionalitas dasar untuk melacak dan mentransfer NFT, sehingga kepemilikan masing-masing sertifikat dapat dilacak secara terpisah [5]

Penelitian ini berfokus pada pengembangan DApp, yaitu jenis aplikasi yang menghosting sebagian dari layanan back-end dan basis data mereka pada jaringan peer-to-peer (p2p) seperti blockchain [6], untuk manajemen sertifikat digital menggunakan NFT berbasis standar ERC-721 di jaringan Ethereum. DApp ini dirancang untuk meningkatkan keamanan, validitas, dan efisiensi dalam manajemen sertifikat digital. Dengan mengadopsi teknologi ini, diharapkan dapat diciptakan sistem manajemen sertifikat digital yang lebih andal dan terpercaya.

Beberapa penelitian yang relevan dengan topik ini telah dilakukan sebelumnya. Misalnya, penelitian [7] mengembangkan sistem sertifikat berbasis NFT untuk perhiasan dan batu permata yang menggarisbawahi penerapan NFT dalam pembuatan sertifikat yang unik, meskipun kasus studinya berbeda dengan penelitian ini. Selain itu, penelitian mereka mengembangkan NFTCert, sertifikat berbasis NFT [8], yang berfokus pada pembuatan smart contract untuk sertifikat NFT. Di bidang pendidikan, penelitian yang dilakukan [9] juga memanfaatkan blockchain untuk pembuatan sertifikat digital, tetapi dalam penelitian tersebut, sertifikat yang digunakan tidak berbentuk NFT.

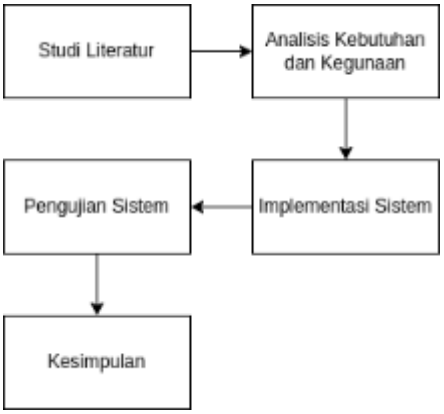
Dengan memperhatikan hasil dari penelitian-penelitian di atas, penelitian ini berusaha untuk memperluas implementasi NFT dalam sertifikat digital, dengan fokus pada manajemen

sertifikat di jaringan Ethereum melalui pengembangan DApp yang aman dan efisien.

II. METODE PENELITIAN

A. Jenis dan Rancangan Penelitian

Peneliti mengembangkan aplikasi DApp untuk manajemen sertifikat digital menggunakan Non-Fungible Tokens (NFT) berbasis Standar ERC-721 di jaringan Ethereum dengan tahapan penelitian seperti yang disajikan pada gambar 1.



Gbr. 1 Rancangan penelitian

B. Analisis Kebutuhan

1. Rincian Fitur

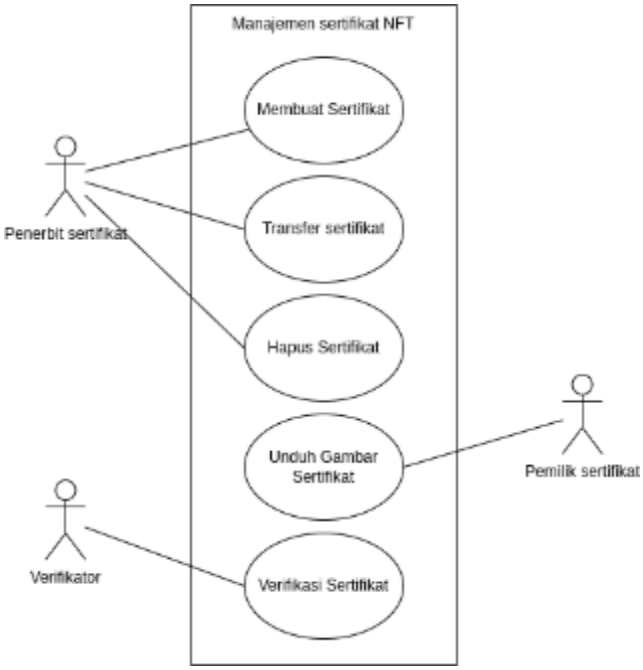
Fitur yang akan dikembangkan pada aplikasi manajemen sertifikat NFT yang akan dibuat seperti yang dijelaskan pada tabel 1.

TABEL I
Rincian Fitur

No	Penjelasan Fitur
1	Membuat sertifikat
2	Transfer sertifikat
3	Verifikasi sertifikat
4	Menghapus sertifikat
5	Unduh gambar sertifikat

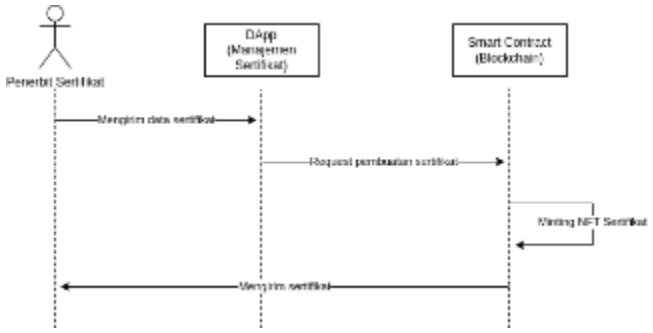
2. Rancangan Implementasi

Gambar 2 menjelaskan use case dari aplikasi manajemen sertifikat NFT yang akan dibuat.



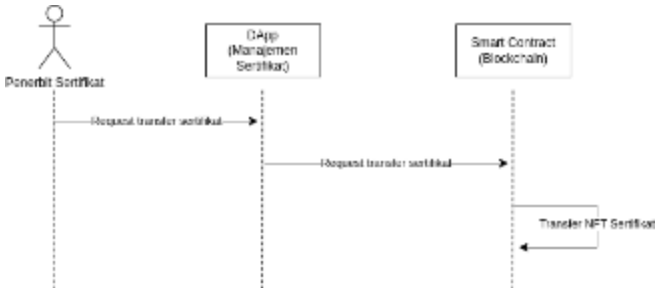
Gbr. 2 Use Case Manajemen Sertifikat NFT

Gambar 3 menjelaskan proses pembuatan sertifikat oleh penerbit sertifikat.



Gbr. 3 Sequence Diagram Pembuatan Sertifikat

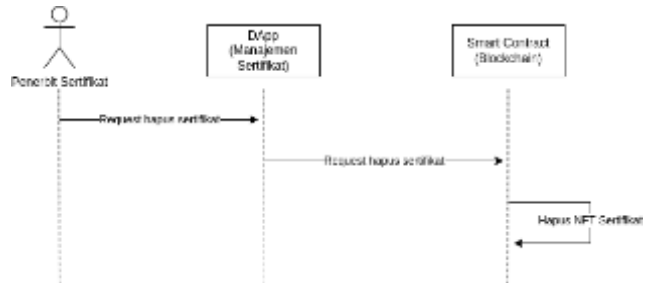
Gambar 4 menjelaskan bagaimana penerbit sertifikat melakukan transfer / memberikan sertifikat kepada pemilik sertifikat.



Gbr. 4 Sequence Diagram Transfer Sertifikat

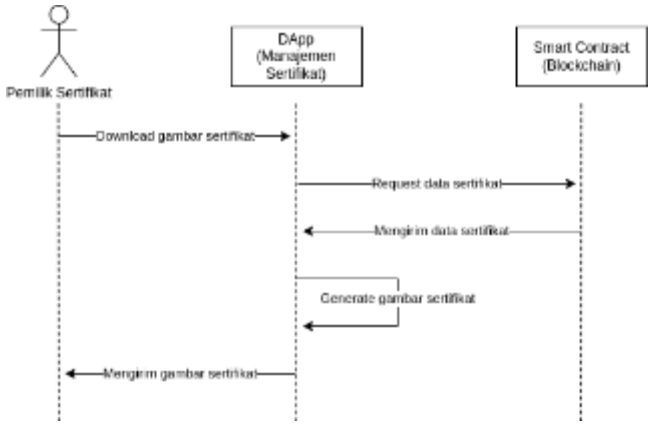
Proses penghapusan sertifikat seperti yang digambarkan pada Gambar 5 tidak benar-benar menghapus sertifikat dari

blockchain, melainkan hanya menandai sertifikat tersebut sebagai dihapus atau dinonaktifkan.



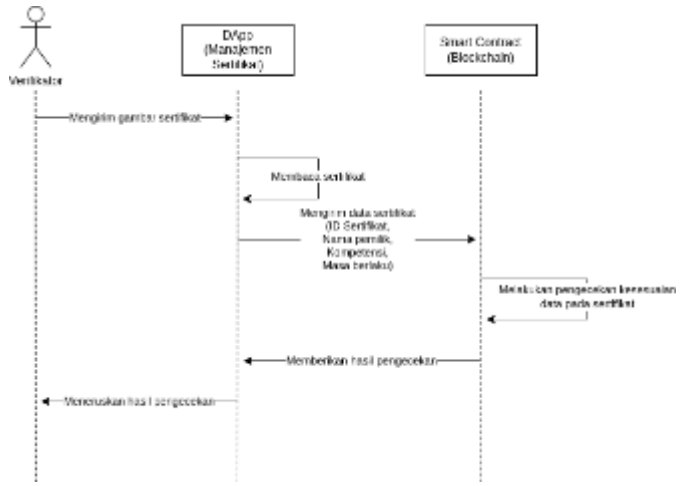
Gbr. 5 Sequence Diagram Hapus Sertifikat

Proses pengunduhan atau pencetakan Sertifikat NFT menjadi gambar dengan format .png dijelaskan pada Gambar 6.



Gbr. 6 Sequence Diagram Unduh Gambar Sertifikat NFT

Gambar 7 menjelaskan bagaimana verifikator dapat mengecek keaslian dan status dari sebuah Sertifikat NFT.



Gbr. 7 Sequence Diagram Verifikasi Sertifikat

3. Pengujiaan

TABEL II
Pengujian Unit

No	Case
1	Membuat sertifikat
2	Transfer sertifikat
3	Verifikasi sertifikat
4	Menghapus sertifikat
5	Unduh gambar sertifikat

Pengujian yang dilakukan dalam penelitian ini dijelaskan pada Tabel II.

III. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan sebuah aplikasi Manajemen Sertifikat NFT berbasis web yang terintegrasi dengan smart contract. Smart contract ini telah dikembangkan oleh peneliti dan diluncurkan di blockchain pada jaringan testnet Sepolia.

A. Studi Literatur

Penelitian ini dimulai dengan melakukan studi literatur yang mencakup jurnal penelitian dan dokumentasi program terkait pengembangan aplikasi berbasis blockchain dan manajemen sertifikat berbasis NFT. Studi ini memberikan wawasan tentang perbandingan antara sertifikat NFT berbasis blockchain dan sertifikat digital konvensional.

1. Perbandingan Sertifikat NFT Berbasis Blockchain dan Sertifikat Digital Konvensional:
   - Keaslian dan Keamanan:
     Sertifikat NFT Berbasis Blockchain: Dicatat dalam blockchain yang terdesentralisasi dan tidak dapat diubah, menjamin keunikan dan keamanan sertifikat dari pemalsuan.
     Sertifikat Digital Konvensional: Disimpan dalam basis data terpusat yang lebih rentan terhadap manipulasi dan serangan cyber.
   - Transparansi:
     Sertifikat NFT Berbasis Blockchain: Semua transaksi dan perubahan status tercatat di blockchain dan dapat diakses publik, meningkatkan transparansi.
     Sertifikat Digital Konvensional: Informasi biasanya hanya dapat diakses oleh entitas tertentu, mengurangi transparansi.
   - Desentralisasi:
     Sertifikat NFT Berbasis Blockchain: Beroperasi pada jaringan peer-to-peer yang terdesentralisasi, tanpa kendali penuh oleh satu entitas.
     Sertifikat Digital Konvensional: Dikelola oleh satu

entitas pusat, membuatnya lebih rentan terhadap serangan atau kerusakan sistem.

B. Analisis Kebutuhan dan Kegunaan

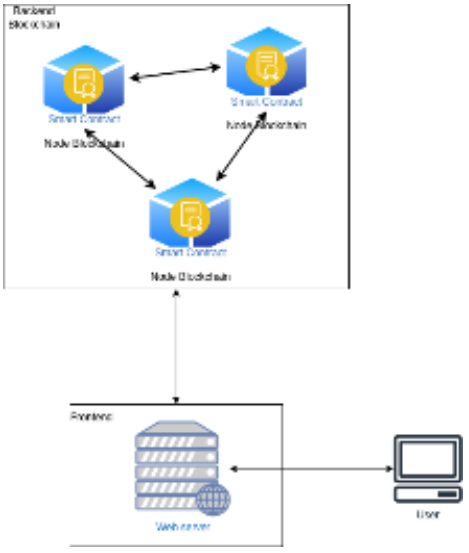
Aplikasi ini dirancang dengan fungsi-fungsi inti yang mendukung manajemen sertifikat NFT. Fungsi utama mencakup autentikasi dan otorisasi pengguna, pembuatan sertifikat NFT, pengiriman sertifikat kepada pengguna, verifikasi keaslian sertifikat, penghapusan atau penonaktifan sertifikat, serta pengunduhan gambar sertifikat NFT.

C. Implementasi Sistem

Implementasi dimulai dengan pengembangan Smart Contract yang berfungsi sebagai backend dari aplikasi manajemen sertifikat NFT. Smart Contract ini diuji menggunakan unit test untuk memastikan fungsionalitasnya. Langkah berikutnya adalah pengembangan antarmuka web yang berfungsi sebagai frontend dari aplikasi tersebut.

1. Arsitektur aplikasi

Seperti yang digambarkan pada gambar 8 arsitektur aplikasi terdiri dari dua bagian utama yaitu backend dan frontend. Backend terdiri dari smart contract berbasis Solidity yang di-deploy di jaringan testnet Sepolia. Solidity sendiri merupakan bahasa pemrograman tingkat tinggi yang berorientasi objek untuk mengimplementasikan smart contract di ethereum [10]. Frontend dikembangkan menggunakan Nuxt 3, yang berinteraksi dengan smart contract melalui library ethers.js.



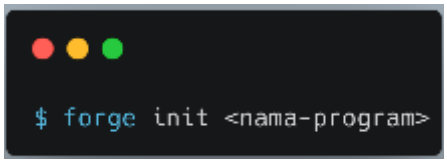
Gbr. 8 Arsitektur aplikasi

2. Smart Contract Solidity

Penulis menggunakan Foundry, sebuah alat pengembangan untuk mempermudah pembuatan smart contract.

Gbr. 9 Menginstall Foundry

Setelah menginstal Foundry seperti pada gambar 9, langkah pertama adalah membuat proyek Foundry dan menginstal library OpenZeppelin, yang diperlukan untuk menggunakan standar ERC-721. Gambar 10 menjelaskan bagaimana membuat proyek Foundry dan gambar 11 adalah command yang digunakan untuk menginstall library OpenZeppelin.



Gbr. 10 Membuat project menggunakan Foundry

Gbr. 11 Menginstal library OpenZeppelin

Untuk memastikan library ini dapat terbaca oleh Foundry, dibuat file remappings.txt yang berisi path instalasi library seperti pada gambar 12.

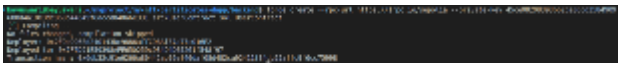
Gbr. 12 Membuat file remappings.txt

Gambar 13 dan 14 adalah smart contract pertama yang dikembangkan. Smart contract tersebut digunakan untuk autentikasi pengguna (UserContract) dan manajemen sertifikat NFT berbasis ERC-721 (NftCertificate).

Gbr. 13 Smart Contract UserContract

Gbr. 14 Smart Contract NftCertificate

Setelah selesai, kedua smart contract ini di-deploy ke jaringan testnet Sepolia menggunakan Foundry, dimulai dengan UserContract, karena NftCertificate memerlukan alamat UserContract saat deployment.



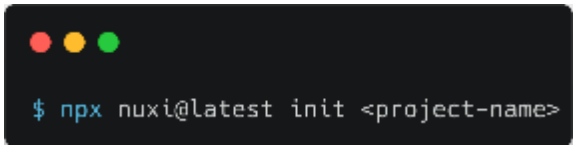
Gbr. 15 Deploy Smart Contract UserContract

Gbr. 16 Deploy Smart Contract NftCertificate

Gambar 15 dan 16 adalah proses deployment smart contract menggunakan foundry.

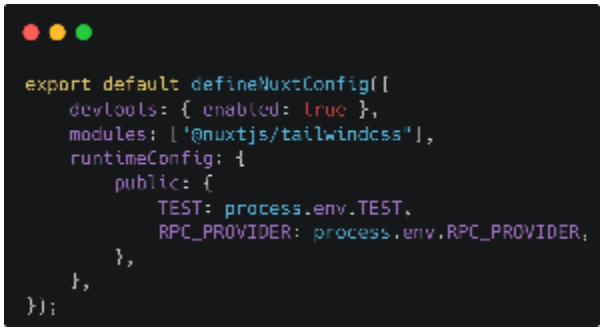
3. Web App

Setelah memastikan smart contract berfungsi dengan baik, tahap berikutnya adalah pengembangan frontend aplikasi berbasis web menggunakan Nuxt 3. Pembuatan proyek dimulai dengan Nuxt 3, diikuti instalasi dependensi yang diperlukan dan konfigurasi Nuxt. Gambar 17, 18, dan 19 menjelaskan bagaimana caranya membuat, menginstall library dan konfigurasi dari project Nuxt yang dibuat.



Gbr. 17 Membuat project Nuxt3

Gbr. 18 Install dependensi



Gbr. 19 Nuxt Config

Aplikasi ini berkomunikasi dengan smart contract melalui ethers.js, library yang digunakan untuk interaksi dengan Ethereum blockchain. Dengan menggunakan alamat dan ABI dari smart contract, fungsi seperti pendaftaran pengguna atau validasi NFT dapat diakses. Fungsi yang menghasilkan transaksi memerlukan signer yang terhubung dengan MetaMask, sementara fungsi view tidak memerlukannya. Gambar 20 merupakan contoh bagaimana cara mengakses fungsi signUp yang memerlukan signer dari user.

Gbr. 20 Mengakses fungsi signUp pada Smart Contract UserContract

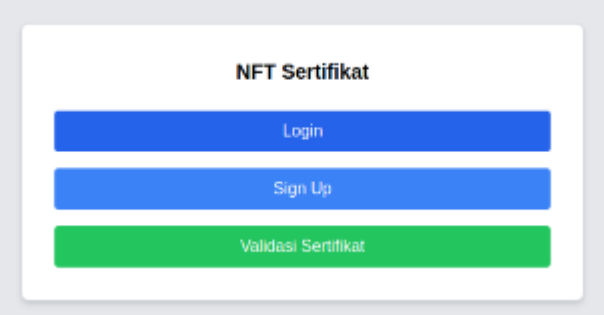
Gbr. 21 Mengakses fungsi validateNFT

Untuk mengakses fungsi yang tidak memerlukan signer dapat dilihat contohnya pada gambar 21.

Setelah integrasi berhasil, halaman web dikembangkan. Halaman utama termasuk:

- Halaman Index

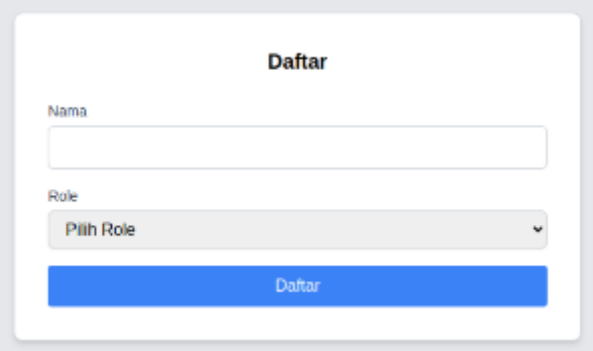
Halaman yang pertama kali dilihat oleh user ketika mengakses aplikasi seperti pada gambar 22.



Gbr. 22 Tampilan awal saat aplikasi diakses

- Halaman Pendaftaran

Untuk melakukan pendaftaran, pengguna dapat mengisi nama dan peran mereka. Tampilannya dapat dilihat pada Gambar 23.

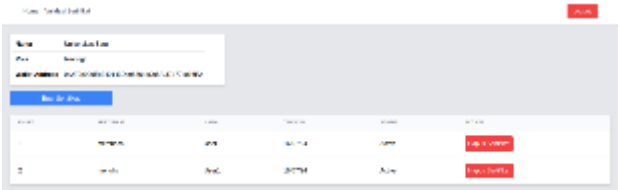


Gbr. 23 Tampilan user mendaftar ke aplikasi

- Halaman Home

Aplikasi ini memiliki dua versi halaman home: versi untuk pemegang/pemilik sertifikat, seperti pada Gambar 24, dan versi untuk penerbit/institusi/lembaga, seperti pada Gambar 25.

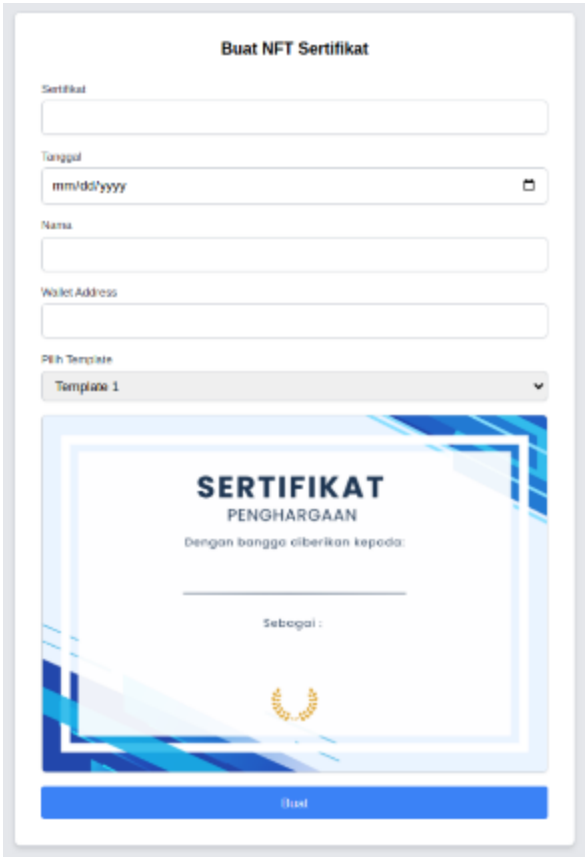
Gbr. 24 Tampilan halaman home pemegang sertifikat



Gbr. 25 Tampilan halaman home institusi / lembaga

- Halaman Pembuatan Sertifikat

Pada halaman ini penerbit dapat melakukan pembuatan sertifikat NFT dengan mengisi formulir seperti pada Gambar 26.

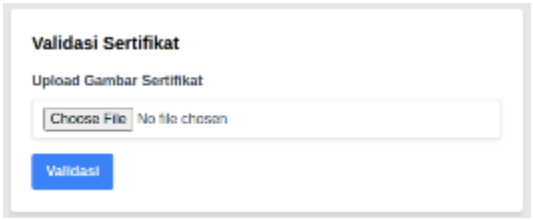


Gbr. 26 Tampilan halaman pembuatan sertifikat NFT

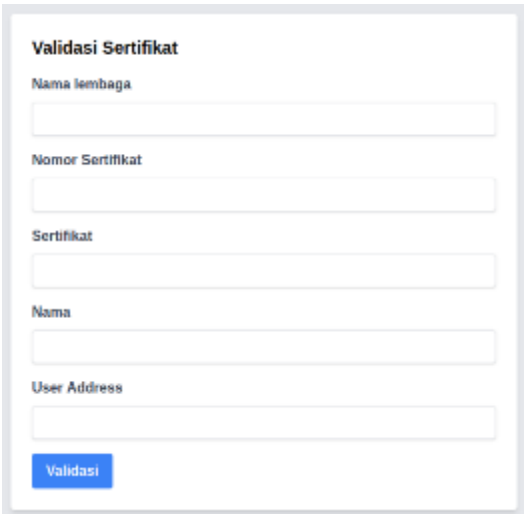
Gbr. 27 Contoh gambar sertifikat

- Halaman Validasi Sertifikat

Terdapat dua halaman untuk validasi sertifikat. Halaman pertama menggunakan gambar, seperti ditunjukkan pada Gambar 28, dan halaman kedua menggunakan metadata sertifikat, seperti ditunjukkan pada Gambar 29.



Gbr. 28 Tampilan halaman validasi sertifikat NFT menggunakan gambar



Gbr. 29 Tampilan halaman validasi sertifikat NFT menggunakan metadata

D. Pengujian Sistem

Pengujian aplikasi dilakukan menggunakan dua metode: white box dan black box.

1. Pengujian White Box / Unit Test

Pengujian white box dilakukan dengan membuat unit test menggunakan Foundry. Setiap unit test dibuat dalam file yang dinamai sesuai dengan smart contract yang diuji, dengan menambahkan .t sebelum ekstensi .sol.

TABEL III
Hasil Pengujian

Smart Contract	Case	Hasil
UserContract	testGetNonExistentUser()	Berhasil dengan gas yang terpakai 18487.
	testSignUpAndSignIn()	Berhasil dengan gas yang terpakai 85719.
	testSignUpInstitution()	Berhasil dengan gas yang terpakai 133351.
NftCertificate	testCreateNFTCertificate()	Berhasil dengan gas yang terpakai 446212
	testDeleteNFTCertificate()	Berhasil dengan gas yang terpakai 393567
	testGetNFTCertificateForLembaga()	Berhasil dengan gas yang terpakai 448653
	testGetNFTCertificateForUser()	Berhasil dengan gas yang terpakai 459508
	testTransferNFTCertificate()	Berhasil dengan gas yang terpakai 479815

Hasil pengujian pada tabel III menunjukkan bahwa semua fungsi dalam smart contract berhasil dijalankan dengan penggunaan gas yang efisien.

2. Pengujian Black Box

Pengujian black box dilakukan melalui interaksi langsung dengan aplikasi web, meliputi skenario penggunaannya seperti pendaftaran, pembuatan sertifikat, dan validasi sertifikat.

Proses pendaftaran pengguna memerlukan penandatanganan transaksi melalui MetaMask. Setelah pendaftaran, pengguna dapat mengakses halaman home yang menampilkan sertifikat yang dibuat atau diterima, tergantung pada peran pengguna (lembaga atau individu).

Fitur penting yang diuji meliputi:

- Daftar Akun: Pengguna berhasil mendaftar dan masuk ke aplikasi dengan identitas yang sesuai.
- Pembuatan Sertifikat NFT: Lembaga berhasil membuat sertifikat NFT dengan metadata yang lengkap.
- Transfer Sertifikat NFT ke Pengguna: Sertifikat NFT berhasil ditransfer dari lembaga ke pengguna yang dituju.
- Penghapusan Sertifikat: Lembaga berhasil menonaktifkan sertifikat, dengan status yang berubah menjadi inactive.
- Pengunduhan Gambar Sertifikat: Pengguna dapat mengunduh gambar sertifikat dalam format .png.
- Validasi Gambar Sertifikat NFT Asli: Validasi gambar sertifikat yang asli berhasil dilakukan.
- Validasi Gambar Sertifikat NFT Palsu: Validasi gambar sertifikat palsu gagal, seperti yang diharapkan.
- Validasi Metadata Sertifikat NFT Asli: Metadata sertifikat yang asli berhasil divalidasi.

- Validasi Metadata Sertifikat NFT Palsu: Validasi metadata sertifikat palsu gagal, memastikan integritas data.
- Validasi Gambar Sertifikat NFT yang Sudah Dihapus: Validasi gagal pada sertifikat yang sudah dihapus, mengonfirmasi statusnya sebagai inactive.

Hasil pengujian black box menunjukkan bahwa seluruh fungsi berjalan sesuai yang diharapkan, kecuali validasi sertifikat palsu yang diatur untuk gagal, memastikan keamanan aplikasi.

IV. PENUTUP

A. Kesimpulan

Penelitian ini berhasil mendemonstrasikan penerapan teknologi blockchain, khususnya Ethereum, sebagai solusi efektif untuk mengatasi tantangan keaslian dan keamanan dalam sertifikat digital. Dengan memanfaatkan teknologi blockchain, sertifikat yang diterbitkan menjadi transparan, tidak dapat diubah, dan dapat diverifikasi secara publik.

Studi ini juga berhasil mengimplementasikan NFT sebagai sertifikat digital menggunakan standar ERC-721, yang memastikan setiap sertifikat bersifat unik, aman, dan tidak dapat dipalsukan. Ini memberikan bukti kepemilikan yang dapat diverifikasi oleh pemilik sertifikat.

Selain itu, pengembangan dan pengujian smart contract yang ditulis dalam Solidity di platform Ethereum menunjukkan bahwa smart contract tersebut berfungsi dengan baik dalam penciptaan, transfer, verifikasi, dan penghapusan sertifikat, sesuai dengan spesifikasi yang ditentukan dan tetap menjaga keamanan yang kuat.

REFERENSI

[1] A. A. Monrat, O. Schelén, and K. Andersson. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. IEEE Access, Vol. 7, pp. 117134-117151. doi: 10.1109/ACCESS.2019.2936094.

[2] Y. -J. Yang and J. -L. Wang. (2023). Non-Fungible Token (NFT) Games: A Literature Review. 2023 International Conference On Cyber Management And Engineering (CyMaEn), Bangkok, Thailand, pp. 251-254. doi: 10.1109/CyMaEn57228.2023.10050961.

[3] Chen, T., Li, Z., Zhu, Y., Chen, J., Luo, X., Lui, J. C. S., ... & Zhang, X. (2020). Understanding Ethereum via Graph Analysis. ACM Transactions on Internet Technology (TOIT), 20(2), 1-32.

[4] Sandhiya, S., Sowbharnika, K., & Preetha, P. (2021). Tokenization of Real World Assets in Ethereum Blockchain Using ERC-721 and ERC-1155.

[5] Cabot-Nadal, M. À., Payeras-Capellà, M. M., Mut-Puigserver, M., & Soto-Fernández, A. (2022, November). Improving the Token ERC-721 Implementation for Selective Receipt: Rejectable NFTs. 2022 6th International Conference on System Reliability and Safety (ICSRS), pp. 243-250. IEEE

[6] Min, T., & Cai, W. (2022). Portrait of Decentralized Application Users: An Overview Based on Large-Scale Ethereum Data. CCF Transactions on Pervasive Computing and Interaction, 4(2), 124-141.

[7] Alnuaimi, Noura & Rr, Al & Madine, Mohammad & Salah, Khaled & Al Breiki, Hamda & Jayaraman, Raja. (2022). NFT Certificates and Proof of Delivery for Fine Jewelry and Gemstones. IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3208698.

[8] Zhao, Xiongfei & Si, Yain Whar. (2021). NFTCert: NFT-Based Certificates With Online Payment Gateway. 538-543. 10.1109/Blockchain53845.2021.00081.

[9] Maulani, Giandari & Gunawan, Gunawan & Leli, Leli & Nabila, Efa & Sari, Windy. (2021). Digital Certificate Authority with Blockchain Cybersecurity in Education. International Journal of Cyber and IT Service Management. 1. 136-150. 10.34306/ijcitsm.v1i1.40.

[10] Solidity Documentation. (2024). Solidity 0.8.25 Documentation. Solidity, https://docs.soliditylang.org/en/v0.8.25/. Diakses pada 1 April 2024.