Jurnal Informatika Universitas Pamulang **ISSN: 2541-1004**
Penerbit: Fakultas Ilmu Komputer Universitas Pamulang **e-ISSN: 2622-4615**
Vol. 10, No. 1, Maret 2025 (32-40) **https://doi.org/10.32493/informatika.v10i1.46055**

Implementasi *Blockchain* sebagai Sistem Validasi dan Arsip Berkas (Sertifikasi dan Ijazah)

Nur Hazbiy Shaffan[1*], Primantara Hari Trisnawan[2], Ananda Fitra Diraja[3], Muhammad Yusuf Affandy[4]

[1234]Fakultas Ilmu Komputer, Universitas Brawijaya, Jl. Veteran, Indonesia, 65144
e-mail: [1]nur.hazbiy@ub.ac.id, [2]prima@ub.ac.id, [3]anandadf@student.ub.ac.id,
[4]myaffandy123@student.ub.ac.id
*Corresponding author

Submitted Date: December 19th, 2024 Reviewed Date: December 27th, 2024
Revised Date: January 16th, 2025 Accepted Date: February 27th, 2025

Abstract

Academic documents such as diplomas and certificates are often the target of forgery, which can reduce the credibility of educational institutions. This study develops a blockchain-based file validation and archiving system to overcome these problems. The methods used include literature studies, system design with a blockchain architecture approach and smart contracts, and implementation of integration with the InterPlanetary File System (IPFS) for digital file storage. The process flow diagram starts from account verification through a digital wallet (eg MetaMask), uploading documents to IPFS to generate a Content Identifier (CID), recording the CID along with metadata on the smart contract, to transaction verification through BlockExplorer. Testing is carried out with two scenarios: (1) testing the functionality of issuing documents by accounts that have access rights and (2) testing security controls that reject submissions from unauthorized accounts. The test results show that the system is able to maintain data integrity, reject unauthorized access, and provide transparent document validation.

Keywords: digital documents; ipfs; blockchain;

Abstrak

Dokumen akademik seperti ijazah dan sertifikat kerap menjadi sasaran pemalsuan, yang dapat menurunkan kredibilitas institusi pendidikan. Penelitian ini mengembangkan sistem validasi dan arsip berkas berbasis teknologi blockchain untuk mengatasi permasalahan tersebut. Metode yang digunakan meliputi studi literatur, perancangan sistem dengan pendekatan arsitektur *blockchain* dan *smart contract*, serta implementasi integrasi dengan *InterPlanetary File System* (IPFS) untuk penyimpanan berkas digital. Diagram alir proses dimulai dari verifikasi akun melalui dompet digital (misalnya MetaMask), pengunggahan dokumen ke IPFS untuk menghasilkan Content Identifier (CID), pencatatan CID beserta metadata pada smart contract, hingga verifikasi transaksi melalui BlockExplorer. Pengujian dilakukan melalui dua skenario: (1) uji fungsionalitas penerbitan dokumen oleh akun yang memiliki hak akses dan (2) uji kontrol keamanan yang menolak submisi dari akun tidak berwenang. Hasil pengujian menunjukkan bahwa sistem mampu menjaga integritas data, menolak akses yang tidak sah, dan menyediakan validasi dokumen secara transparan.

Kata kunci: dokumen digital, ipfs, blockchain

1. Pendahuluan

Pemalsuan dokumen akademik seperti ijazah sering terjadi, terutama pada dokumen fisik yang mencakup tindakan pemalsuan maupun pengubahan isi dokumen (Netto & Carter, 2013; Kim, 2013). Para pelaku kejahatan memanipulasi dokumen cetak agar tampak asli sehingga dapat menipu pihak penerima untuk memperoleh keuntungan. Sebagai contoh, di Amerika Serikat, dua tersangka terbebas dari hukuman dikarenakan adanya perintah pengadilan palsu (Netto & Carter, 2013), selain itu terdapat juga kasus imigran ilegal dari India yang pernah menggunakan izin kunjungan sosial palsu untuk

ISSN: 2541-1004
e-ISSN: 2622-4615
https://doi.org/10.32493/informatika.v10i1.46055

mencari pekerjaan di Malaysia (Kim, 2013). Potensi kecurangan ini muncul dikarenakan meningkatnya transisi penggunaan dokumen fisik ke dokumen elektronik yang menggunakan tanda tangan digital (*digital signature*).

Saat ini, banyak perusahaan penyedia jasa pengesahan sertifikat yang bekerja sama dengan instansi pemerintah dalam penerbitan sertifikat elektronik. Sertifikat ini memuat informasi pribadi, seperti nama lengkap, nomor induk kependudukan, dan alamat. Jika informasi tersebut disalahgunakan, pemilik sertifikat berpotensi mengalami kerugian. Oleh karena itu, penting adanya perlindungan hukum terhadap data pribadi yang tercantum dalam dokumen digital. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Pasal 26 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) secara eksplisit mengatur mengenai larangan penggunaan data pribadi tanpa persetujuan, serta menetapkan sanksi pidana terhadap pelanggaran penyalahgunaan data pribadi (Ardhana & Sutama, 2022; Wulandari & Purnama, 2023).

Untuk mengatasi permasalahan ini, penelitian ini memanfaatkan teknologi *blockchain* yang menawarkan penyimpanan data secara terdistribusi, transparan, dan tidak dapat diubah (immutable). Konsep *blockchain* diperkenalkan pada tahun 2008 oleh Satoshi Nakamoto yang dikenal dengan sistem keuangan elektronik yang disebut *Bitcoin*. Saat ini, teknologi *blockchain* telah berkembang pesat dan diadopsi oleh berbagai perusahaan, seperti implementasi teknologi ini pada bisnis perbankan oleh Weizhong Bank milik Tencent pada September 2016. (Wei et al., 2020).

Dalam kasus dokumen digital, dokumen yang disimpan pada sistem *blockchain* memiliki jejak digital yang sulit dimanipulasi, karena setiap transaksi diverifikasi melalui mekanisme konsensus yang melibatkan banyak pihak (Belotti et al., 2019). Pada penelitian sebelumnya, sistem verifikasi integritas dokumen cetak konvensional seperti penggunaan barcode terbukti mampu membantu proses autentikasi dan mendeteksi pemalsuan dokumen, tetapi masih memiliki kelemahan karena bergantung pada sistem penyimpanan terpusat yang rentan terhadap manipulasi data (Husain, Bakhtiari, & Zainal, 2014). Permasalahan ini dapat diselesaikan menggunakan teknologi *blockchain* dengan memanfaatkan konsep *Non-Fungible Token* (NFT) (Wang et al., 2021). NFT adalah token digital unik yang dihasilkan dan dikendalikan oleh *smart contract* pada *blockchain*. Setiap NFT memiliki kode identifikasi unik yang tidak bisa diduplikasi, sehingga setiap dokumen elektronik seperti sertifikat atau ijazah yang diwakili oleh NFT tersebut menjadi mudah diverifikasi keasliannya. NFT menyimpan *metadata* penting, seperti informasi penerbit, tanggal penerbitan, serta tautan *Content Identifier* (CID) ke dokumen asli yang disimpan secara terdesentralisasi dalam sistem *InterPlanetary File System* (IPFS). IPFS dalam penelitian ini berfungsi sebagai penyimpan dokumen yang aman dan terdesentralisasi, sementara *blockchain* dengan menyimpan CID dapat menyediakan rekaman transaksi yang transparan dan tidak dapat diubah, sehingga setiap upaya pemalsuan dapat segera terdeteksi (Benet, 2014; Trautwein et al., 2022). Pengembangan sistem dengan menggabungkan NFT dan IPFS ini diharapkan dapat menjaga dokumen elektronik agar tetap otentik, tidak dapat dimanipulasi, dan dapat diverifikasi keabsahan datanya secara transparan oleh berbagai pihak.

2. Metode Penelitian

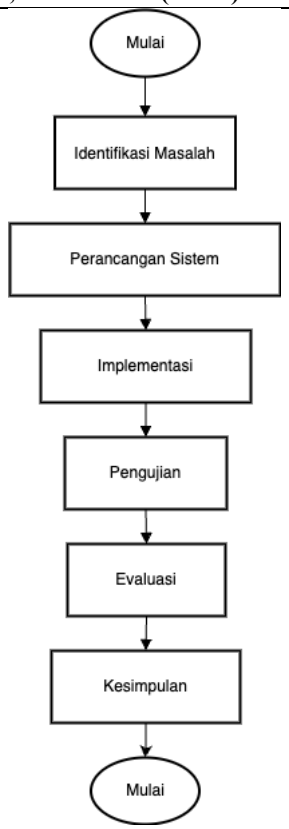
Dalam proses pembuatan sistem, peneliti menggunakan tahapan metode penelitian sebagai berikut:

Secara keseluruhan, tahapan metode penelitian seperti yang ditunjukkan pada Gambar 1 disusun untuk memudahkan proses penyelesaian penelitian. Berikut adalah penjabaran detail dari setiap tahapannya.

2.1 Identifikasi Masalah

Dalam penelitian ini, permasalahan yang diangkat berkaitan dengan kasus pemalsuan dokumen. Identifikasi masalah dalam studi kasus pemalsuan dokumen akademik mengungkap kelemahan sistem verifikasi tradisional yang rentan terhadap manipulasi. Penelitian oleh Cardenas Quispe dan Pacheco (2025) dan Zhao et al. (2021) menunjukkan bahwa metode verifikasi konvensional sering kali gagal mendeteksi upaya pemalsuan, sehingga mengakibatkan penurunan kredibilitas institusi pendidikan

ISSN: 2541-1004
e-ISSN: 2622-4615
https://doi.org/10.32493/informatika.v10i1.46055



Gambar 1. Diagram alir metode penelitian

Studi-studi tersebut menyoroti bahwa ketergantungan pada sistem terpusat dan minimnya mekanisme keamanan yang efektif merupakan faktor utama yang memungkinkan terjadinya pemalsuan. Dengan mengidentifikasi masalah ini, penelitian ini memanfaatkan teknologi *blockchain* dan IPFS yang dapat meningkatkan integritas dan keaslian dokumen akademik secara terdesentralisasi.

2.2 Perancangan Sistem

Desain arsitektur sistem dilakukan dengan mengintegrasikan blockchain dan smart contract pada platform Consensys Quorum (Nelson, 2021). Perancangan sistem pada penlitian ini terdiri dari beberapa tahapan sebagai berikut:

2.2.1 Rekayasa Kebutuhan

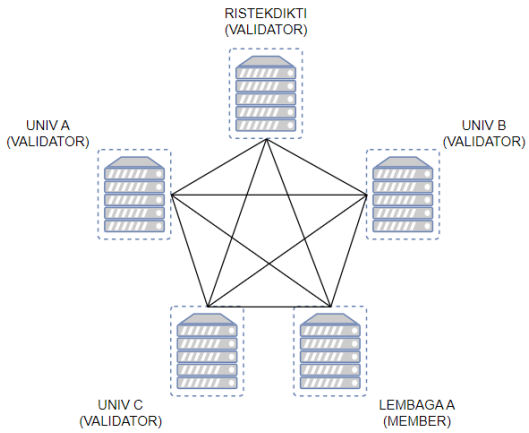
Tabel berikut menjelaskan daftar kebutuhan yang digunakan untuk pengembangan rancang bangun infrastruktur *blockchain* sebagai sistem penyimpanan dokumen akademis.

Table 2.1. Tabel Kebutuhan Perangkat

Kebutuhan	Perangkat Lunak/Keras
Blockchain Node	Perangkat Keras: • Komputer Perangkat Lunak: • Ansible • Docker Container
Block Explorer	Perangkat Keras: • Komputer Perangkat Lunak: • Blockscout • Docker Container
Website	Perangkat Keras: • Komputer Perangkat Lunak: • Sistem *front-end*

2.2.2 Perancangan Infrastruktur

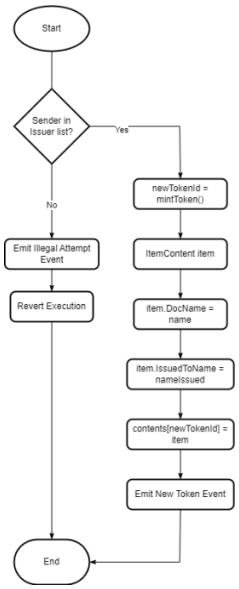
Perancangan sistem merupakan tahap awal untuk membangun lingkungan sistem yang diharapkan, dimulai dari proses persiapan lingkungan dengan menggunakan platform Consensys GoQuorum, pengembangan kode *smart contract* dilakukan dengan bahasa pemrograman yang didukung langsung oleh Ethereum Virtual Machine (EVM), yaitu Solidity. Struktur anggota dari peserta jaringan Quorum untuk penelitian ini adalah terdapat empat (4) *nodes* yang berperan sebagai *validator node* untuk proses *consensus*, dan satu (1) node yang berperan sebagai *member node* untuk pengaksesan data *ledger* secara lokal. Penelitian ini juga menggunakan *blockchain explorer* bernama *Blockscout* untuk memantau informasi historis dari seluruh catatan yang ada pada jaringan *blockchain* secara *real-time*.



Gambar 2. Diagram interkoneksi jaringan quorum

Proses penerbitan akan dilakukan pada suatu *smart contract* sebagai media penyimpanan dan data historis dokumen dengan mengikuti spesifikasi ERC-721. Pada observasi ini, kita

akan menggunakan beberapa *library* dari OpenZeppelin sebagai basis dasar *smart contract* tersebut, kemudian diikuti dengan diagram alir untuk fungsi penerbitan dokumen dalam bentuk NFT sebagai berikut:



Gambar 3. Diagram alir *smart contract*

2.2.3 Perancangan Kebutuhan Fungsional Sistem

Sebelum melakukan pengembangan dari *smart contract*, dirancang beberapa kebutuhan fungsional yang didefinisikan yaitu sistem hanya akan menerima submisi penerbitan dokumen dari akun yang memiliki hak penerbit, dimana pada saat adanya percobaan submisi dari pihak yang tidak berwenang, sistem akan menolak submisi tersebut, sehingga diharapkan dapat menjaga validitas data yang lebih baik. Penentuan serta perubahan dari pihak-pihak yang memiliki hak tersebut juga dapat diatur pada sistem dengan memanfaatkan *smart contract* sehingga kondisi dapat disimpan secara terdesentralisasi.

2.2.4 Otomatisasi Implementasi Layanan Sistem

Sistem *blockchain* akan diterapkan dengan menggunakan Ansible yang berperan dalam melakukan otomasi penerapan infrastruktur dan kerangka kerja yang dibutuhkan dalam penelitian ini.

2.3 Skenario Pengujian dan Analisis Hasil

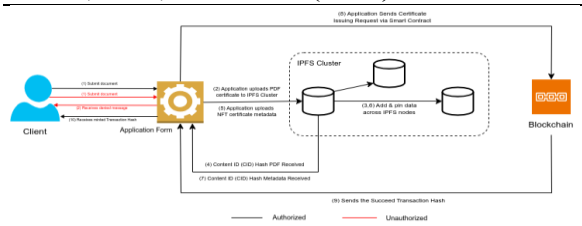
Pada bagian pengujian dan analisis setelah implementasi sistem adalah melakukan pengujian dan analisis hasil. Sistem yang dibangun berfungsi untuk menyimpan data dokumen akademik dalam bentuk *non-fungible token (NFT)* yang dapat diuji keabsahannya walaupun pihak yang terlibat dalam jaringan *blockchain* ini lebih dari satu pihak yang berbeda. Dalam proses penyimpanan, terdapat beberapa variabel yang diperhatikan, yaitu durasi waktu yang dibutuhkan untuk suatu dokumen dapat menjadi transaksi yang sah dalam sistem, dan pengujian fungsionalitas yang akan menguji keabsahan data apabila terdapat submisi dokumen palsu serta proses perubahan anggota *validator* pada saat sistem berjalan.

3. Implementasi

3.1 Sistem Penyimpanan Dokumen

Sistem penyimpanan dokumen seperti berkas PDF akan diunggah pada sistem IPFS dalam bentuk sebuah *hash* CID yang akan disisipkan sebagai sebuah *metadata* pada NFT sertifikat yang diterbitkan pada *smart contract*. Dan pada saat proses perolehan sertifikat yang diterbitkan dapat diakses pada *metadata* NFT sertifikat pada sistem *blockchain*.

Sebelum melakukan proses submisi dokumen, pengguna diwajibkan untuk menghubungkan akun dengan penyedia dompet Web3 seperti MetaMask sebagai otentikasi identitas. Selanjutnya, pada saat proses *submit* dimulai, aplikasi akan melakukan verifikasi otorisasi dengan mengacu pada data *role* yang tersimpan pada *smart contract*. Jika akun dompet yang terhubung memiliki *role* sebagai penerbit, maka aplikasi akan memulai proses penerbitan dokumen. Sebaliknya, jika akun tersebut tidak memiliki *role* tersebut, maka sistem akan menampilkan pesan penolakan yang menyatakan bahwa akun tersebut tidak memiliki izin (Wang et al., 2018). Setelah proses verifikasi akun selesai, aplikasi akan menyimpan berkas dokumen PDF ke sistem IPFS, yang akan menghasilkan sebuah *content identifier* (CID) untuk mengakses berkas tersebut. Setelah CID dari PDF tersebut telah diterbitkan, sistem akan membuat sebuah metadata berbasis JSON yang akan diunggah ke sistem IPFS yang dimana nilai CID dari *metadata* tersebut akan disimpan sebagai sebuah tautan URI token sertifikat tersebut pada *smart contract* di *blockchain*, yang pada akhirnya memanggil fungsi penerbitan token sertifikat tersebut dengan parameter yang telah disebutkan sebelumnya, yang akan menghasilkan sebuah *hash* transaksi yang nantinya diberikan kembali ke klien dan disimpan sebagai transaksi yang sah.



Gambar 4. Diagram alir mekanisme penerbitan dokumen

3.2 *Smart Contract*

Terdapat beberapa fungsi yang dirancang pada smart contract, yaitu pemberian dan pelepasan suatu role kepada suatu akun dompet, melakukan penerbitan token yang sah, serta perolehan data dari ID token yang telah diterbitkan. Terdapat dua (2) parameter inisial yang didefinisikan pada saat instalasi awal *smart contract*, yaitu parameter admin dan pengesah, yang menentukan kondisi awal dari akun-akun yang dapat melakukan pengesahan serta perubahan anggota akun yang dapat melakukan penerbitan dokumen.

Sistem *smart contract* yang dikembangkan memiliki tingkatan peran yang didefinisikan, yaitu peran administrator yang memiliki wewenang dalam melakukan perubahan anggota dari peran penerbit Selanjutnya terdapat peran penerbit, yang berhak dalam melakukan penerbitan dokumen baru. Sistem *smart contract* ini memiliki beberapa fungsi yang dikembangkan guna memenuhi kebutuhan fungsional yang disebutkan sebelumnya.

Didalam sistem *smart contract*, terdapat fungsi *safeMintDocument*() yang fungsi utama dari implementasi sistem. Fungsi ini bertugas untuk melakukan penerbitan dokumen menjadi bentuk *Non-Fungible Token (NFT)* yang dapat diverifikasi pada *block explorer* serta dokumen yang diasosiasikan dengan NFT yang telah diterbitkan. Pada proses *safeMintDocument(),* beberapa langkah dilakukan untuk memastikan bahwa token NFT yang baru dibuat valid dan aman. Berikut adalah detail langkah-langkahnya:

- Validasi Akses dan Otorisasi:

Fungsi safeMint memeriksa terlebih dahulu apakah pemanggil (caller) memiliki hak untuk melakukan minting, sehingga hanya akun yang berotorisasi yang dapat menerbitkan token baru.

- Penentuan Token ID Unik:

Sistem menghasilkan *token ID* yang unik untuk setiap token yang akan diterbitkan. Ini penting untuk menjamin bahwa setiap NFT memiliki identitas yang tidak dapat diduplikasi.

- Pembuatan Token:

Fungsi internal *_safeMint*() dipanggil untuk membuat token baru. Versi safeMint memastikan bahwa jika token dikirim ke alamat kontrak, kontrak tersebut dapat menerima token dengan benar sesuai standar ERC721.

- Validasi Penerima Token:

SafeMint melakukan pengecekan tambahan dengan memanggil fungsi *_checkOn ERC721Received().* Langkah ini memastikan bahwa jika token dikirimkan ke *smart contract*, kontrak tersebut akan meng-implementasikan interface *ERC721Receiver* sehingga token tidak hilang.

- Penyimpanan Metadata:

Metadata token, dalam hal ini berupa URI yang menunjuk ke lokasi berkas di IPFS, disimpan dalam smart contract. Hal ini memberikan informasi lengkap tentang token, seperti detail dokumen yang terhubung, sehingga keasliannya dapat diverifikasi.

- Emisi Event:

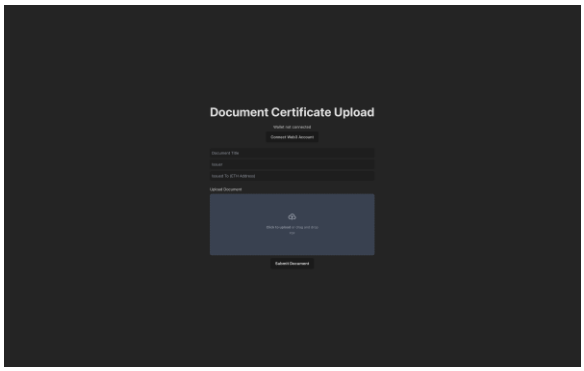
Setelah token berhasil dibuat, event token minted dipicu untuk mencatat transaksi pembuatan token di blockchain, sehingga memudahkan pelacakan dan audit.

Selanjutnya terdapat fungsi *tokenURI()* yang akan memberikan tautan ke *metadata* dari NFT yang terkait, dengan parameter yang diberikan kepada fungsi tersebut dengan suatu ID *token*, sehingga pengguna dapat melihat informasi dari dokumen dari ID *token* yang bersangkutan.

3.3 Website

Proses pembuatan transaksi ini dilakukan melalui *website* agar mempermudah pengguna dalam mengoperasikan sistem. Fitur yang ada dalam *website* adalah untuk mengunggah berkas dalam bentuk *form,* serta untuk mengakses berkas yang telah didapatkan dari fungsi *tokenURI()* dengan mengakses URI yang terdapat pada *metadata* berkas tersebut melalui IPFS. Selain itu pada *website* juga terdapat mekanisme untuk terhubung ke *wallet* melalui *web3*, sehingga website dapat mengautentikasi pengguna dan mengecek apakah pengguna memiliki akses sistem atau tidak. Dokumen seperti berkas PDF akan diunggah pada sistem IPFS dalam bentuk sebuah *hash* CID yang akan disisipkan sebagai

sebuah *metadata* pada NFT sertifikat yang diterbitkan pada *smart contract*. *Metadata* ini nantinya akan diakses oleh fungsi *tokenURI()* seperti yang sudah disampaikan pada subbab 3.2.



Gambar 5. Tampilan *website* untuk mengakses sistem

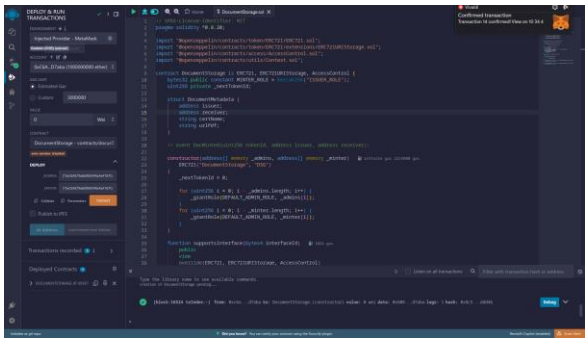
4. Hasil dan Pembahasan

4.1 Skenario

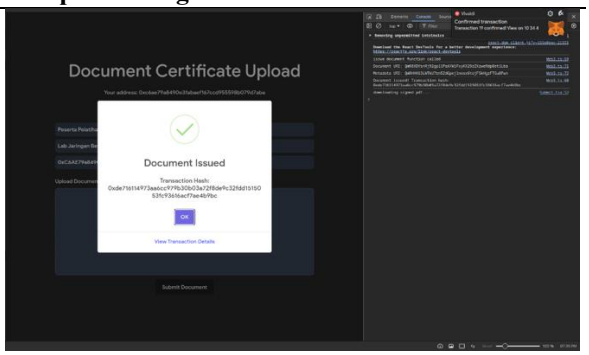
Tahap pra-pengujian yang dilakukan adalah melakukan penerapan kode *smart contract* dengan kebutuhan yang telah disebutkan pada bab sebelumnya. Penelitian ini akan menguji respons serta mekanisme sistem pada kasus percobaan submisi dokumen pada akun *wallet* yang memiliki hak penerbitan serta submisi yang berasal dari akun yang tidak berwenang. Skenario pengujian ini diharapkan bahwa sistem dapat memberikan respon yang sesuai yang diharapkan pada kebutuhan fungsional sistem.

4.2 Hasil

Proses inisiasi *smart contract* berhasil diterapkan pada sistem *blockchain* sebagai sistem yang digunakan dalam penyimpanan integritas data berdasarkan Gambar 6. Terdapat beberapa parameter yang diberikan pada proses penerapan kode pada sistem *blockchain*, yaitu parameter `admin` yang memiliki wewenang dalam mengatur akun yang berhak dalam penerbitan dokumen.

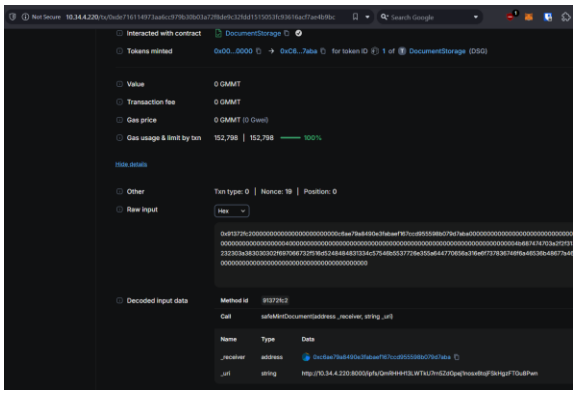


Gambar 6. Penerapan *smart contract* pada *blockchain*



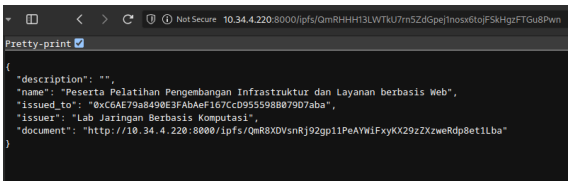
Gambar 7. Sistem berhasil menerbitkan dokumen

Selanjutnya, saat submisi dokumen dilakukan oleh pihak yang berwenang, dokumen PDF dan *metadata* dokumen yang dikirim akan disimpan pada sistem IPFS. Selanjutnya, sistem dapat mengirimkan respons pesan berupa *hash* transaksi yang berkaitan dengan submisi tersebut, dan transaksi tersebut dapat dilihat pada sistem *block explorer* untuk melihat datanya dengan lebih detail.



Gambar 8. Detail transaksi dokumen yang terbit

Pada transaksi penerbitan yang telah dilakukan, seluruh pengguna dapat mengakses *metadata* dari token dokumen yang telah diterbitkan pada *smart contract*. *Metadata* ini tersimpan pada IPFS dan berisikan data sebagai berikut:

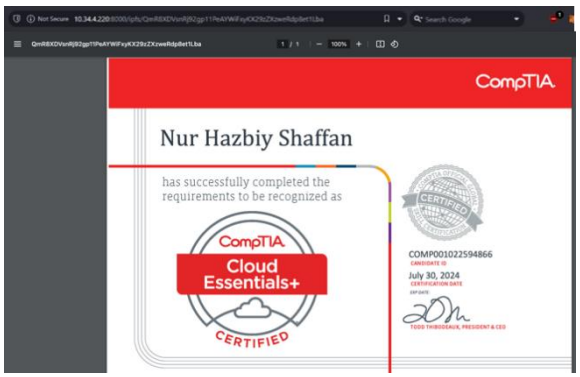


Gambar 9. *Metadata* dari token dokumen

Selain digunakan untuk menghubungkan data yang tersimpan pada *blockchain* dengan arsip digital yang disimpan pada IPFS, *metadata*

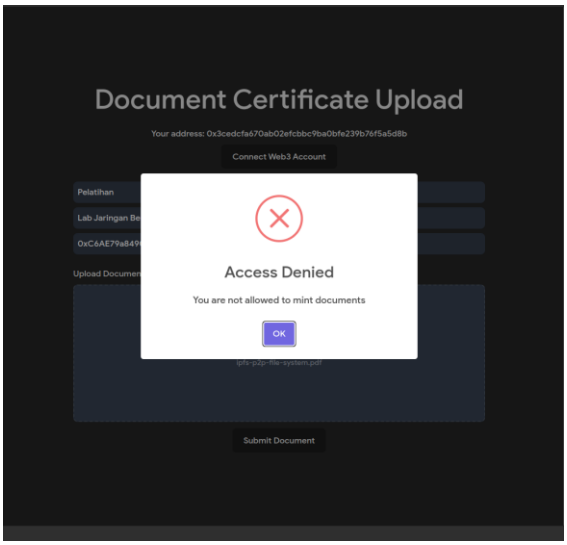
dapat juga digunakan untuk menjaga keabsahan tetap terjaga dikarenakan data yang tersimpan pada sistem *blockchain* tidak dapat dimanipulasi layaknya penyimpanan data konvensional seperti pada sistem *database,* data dapat dimanipulasi dengan mengubah data yang tersimpan pada *datanase*. Pada sistem ini, hal tersebut tidak dapat dilakukan dikarenakan semua data telah tersimpan pada *block-block*, dan data yang tersimpan akan terlihat jelas seperti pada Gambar 8 dan 9.

Apabila ada entitas yang berhasil mendapatkan otoritas untuk membuat transaksi dan ingin memalsukan data, maka entitas tersebut harus menerbitkan dokumen palsu tersebut sebagai transaksi baru, sehingga semua *metadata* seperti pada Gambar 8 dan 9 akan tersimpan secara permanen, sehingga akan mudah mengetahui siapa yang memalsukan data dan kapan pemalsuan data tersebut dilakukan. Pengguna dapat mengakses dokumen melalui URI yang didefinisikan pada *metadata*. Artinya, untuk memalsukan data tanpa melalui submisi baru, maka pelaku pemalsuan data perlu memanipulasi *metadata* tersebut. Hal ini sangat sulit dilakukan dikarenakan *smart contract* tidak dapat melakukan manipulasi dari *metadata* setelah dokumen berhasil diterbitkan. Artinya, pelaku perlu memanipulasi *metadata* di semua *node* yang menyimpan data *blockchain,* serta merekonstruksi semua blok dari blok yang dimanipulasi hingga blok terakhir, sebelum blok yang telah dimanipulasi tersebut dianggap valid oleh sistem.



Gambar 10. Dokumen yang disimpan pada *metadata token*

Skenario pengujian selanjutnya adalah pengujian akun yang tidak memiliki otoritas untuk melakukan submisi dokumen. Pada skenario ini, sistem akan memberikan pesan penolakan bahwa akun tersebut tidak diizinkan. Respon ini membuktikan bahwa sistem dapat menjaga kontrol akses dari akun yang tidak memiliki izin dalam melakukan penerbitan dokumen.



Gambar 11. Sistem menolak submisi dari pihak tidak berwenang

6. Kesimpulan

Penelitian ini berhasil mengimplementasikan sistem penyimpanan dokumen secara terdesentralisasi dengan memanfaatkan teknologi *blockchain* dan IPFS yang diintegrasikan melalui antarmuka *website*. Implementasi dilakukan melalui beberapa tahap, yaitu persiapan infrastruktur *blockchain* menggunakan platform *Consensys GoQuorum*, pengembangan smart contract menggunakan bahasa pemrograman Solidity yang kompatibel dengan *Ethereum Virtual Machine* (EVM), serta pengembangan form submisi dokumen pada website yang langsung berinteraksi *dengan smart contract* di jaringan blockchain.

Berdasarkan hasil implementasi dan pengujian, sistem terbukti mampu menjaga integritas data dengan menerapkan mekanisme kontrol akses yang ketat. Sistem ini berhasil mencegah pengiriman dokumen oleh pihak yang tidak berwenang, sehingga integritas, keamanan, dan keabsahan dokumen digital terjamin secara transparan dan terdesentralisasi.

Daftar Pustaka

Ardhana, I. M. A. S., & Sutama, I. K. (2022). Tinjauan yuridis terhadap perlindungan data pribadi dalam sistem elektronik di

Indonesia. Jurnal Ilmu Sosial dan Humaniora, 11(4), 453–460. https://doi.org/10.22225/jish.11.4.2022.453-460

Belotti, M., Bozic, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. IEEE Communications Surveys & Tutorials, 21(4), 3796–3838. https://doi.org/10.1109/COMST.2019.2928178

Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. arXiv:1407.3561. https://doi.org/10.48550/arXiv.1407.3561

Cardenas Quispe, M. A., & Pacheco, A. (2025). Blockchain ensuring academic integrity with a degree verification prototype. Scientific Reports, 15, Article 9281. https://doi.org/10.1038/s41598-025-93913-6

Netto, J., & Carter, C. J. (2013, October 18). Official: Forged documents used in prison break from Fla. prison. Channel News Network (CNN). Available at: http://edition.cnn.com/2013/10/16/us/florida-inmates-mistakenly-freed/v

Kim, C. B. (2013, November 05). Johor immigration busts syndicate producing fake social visit passes. New Straits Times. Available at: http://www.nst.com.my/latest/johor-immigration-busts-syndicate-producing-fake-social-visit-passes-1.392796

Husain, A., Bakhtiari, M., & Zainal, A. (2014). Printed Document Integrity Verification Using Barcode. Jurnal Teknologi, 70(1). https://doi.org/10.11113/jt.v70.2857

Nelson, M. (2021). What is Consensys Quorum? Diakses dari https://consensys.io/blog/what-is-consensys-quorum

Trautwein, D., Raman, A., Tyson, G., Castro, I., Scott, W., Schubotz, M., Gipp, B., & Psaras, Y. (2022). Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web. Diakses dari https://doi.org/10.48550/arXiv.2208.05877

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. Diakses dari https://doi.org/10.48550/arXiv.2105.07447

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F.-Y. (2018). An Overview of Smart Contract: Architecture, Applications, and Future Trends. Dalam 2018 IEEE Intelligent Vehicles Symposium (IV) (hlm. 108–113). IEEE. https://doi.org/10.1109/IVS.2018.8500488

Wei, P., Wang, D., Zhao, Y., Tyagi, S.K.S., & Kumar, N. (2020). Blockchain Data-based Cloud Data Integrity Protection Mechanism. Future Generation Computer Systems, 102, 902–911. https://doi.org/10.1016/j.future.2019.09.028

Buterin, V. (2014). A Next-generation Smart Contract and Decentralized Application Platform. Diakses dari https://ethereum.org/en/whitepaper/

Wulandari, T. R., & Purnama, S. D. (2023). Perlindungan hukum terhadap data pribadi pengguna aplikasi digital dalam perspektif UU ITE dan UU PDP. *Jurnal Novum*, 10(1), 12–20. https://ejournal.unesa.ac.id/index.php/novum/article/view/58097

Zhao, Z., Chen, W., Liu, X., & Xu, Y. (2021). Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. Journal of Medical Systems, 45(9), 1–13. https://doi.org/10.1007/s10916-021-01772-5