Jurnal Ilmiah Informatika Komputer, 28(2): 100-111.
Doi: https://doi.org/10.35760/ik.2023.v28i2.8958

PERANCANGAN DAN IMPLEMENTASI SMART CONTRACT PADA SISTEM VERIFIKASI DOKUMEN BERBASIS ZERO KNOWLEDGE PROOF (ZKP) PADA BLOCKCHAIN POLYGON

[1] Muhammad Fadhil Abidin, [2]Avinanta Tarigan, [3]Lely Prananingrum*
[1]Fakultas Teknologi Industri Universitas Gunadarma,
[2,3]Fakultas Ilmu Komputer Universitas Gunadarma
Jl. Margonda Raya 100, Depok, Jawa Barat
[1]abidinfadhil@gmail.com, [2]avinanta@staff.gunadarma.ac.id, [3]lely_p@staff.gunadarma.ac.id
**) Penulis korespondensi*

Abstrak

Blockchain merupakan sistem terdesentralisasi yang terbuka yang dapat dimanfaatkan untuk melakukan pelacakan dan verifikasi keaslian dokumen. Sifat keterbukaan tersebut menjadi masalah jika isi dari dokumen bersifat rahasia atau dilindungi oleh undang-undang perlindungan data pribadi. Dalam penelitian ini, sebuah sistem verifikasi dokumen berbasis Blockchain dirancang dengan memanfaatkan algoritma ZKP (Zero Knowledge Proof) yang diimplementasikan dalam sebuah Smart Contract pada jaringan Blockchain Polygon. Algoritma ZKP melindungi informasi yang bersifat rahasia tetapi dapat diverifikasi kebenaran dan keasliannya oleh pihak yang berkepentinga tanpa menguak informasi tersebut. Penelitian ini melibatkan perancangan smart contract yang terdiri dari fungsi-fungsi untuk mengatur proses verifikasi dokumen, serta implementasi sistem verifikasi dokumen yang terintegrasi dengan Smart Contract. Hasil penelitian menunjukkan bahwa sistem yang dibangun dapat meningkatkan keamanan proses pelacakan dokumen dengan tidak menguak isi dokumen yang bersifat rahasia dan dilindungi oleh undang-undang.

***Kata Kunci**: Blockchain, Dokumen, ZKP, Kriptografi, Verifikasi*

Abstract

Blockchain is open decentralized systems which can be used to track changes and verify the authenticity of digital formal documents. The nature of this openness becomes a problem if the part of contents of the document are confidential or protected by personal data protection laws. In this research, a document verification system was designed using the ZKP algorithm which is implemented in a Smart Contract deployed on the Polygon Blockchain network. The ZKP algorithm protects data that is confidential but can be verified for its truth and authenticity without disclosing the data to other parties. This research involves the design of a smart contract which consists of functions to manage the document verification process, as well as the implementation of a document verification system that is integrated with the Smart Contract. The results of the research show that the system built can improve the security of the document tracking process by not disclosing the contents of documents that are confidential and protected by law.

***Keywords**: Blockchain, Documents, ZKP, Cryptography, Verification*

PENDAHULUAN

Dokumen memiliki peranan penting dalam berbagai aspek kehidupan, baik dalam bisnis, pemerintahan, maupun kehidupan sehari-hari. Ijazah dan Transkrip Nilai adalah contoh dokumen harus dapat dibuktikan keasliannya agar pemangku kepentingan percaya terhadap isi dokumen tersebut. Keaslian dokumen dan salinannya secara hukum dapat dibuktikan menggunakan dengan tanda tangan dan cap (legalisir). Menurut UU ITE [1], pembuktian keaslian dokumen digital dapat menggunakan rangkaian proses yang melibatkan kriptografi yang disebut tanda tangan elektronik (*digital signature)* [2]. Teknologi Blockchain akhir-akhir ini telah digunakan untuk membuktikan keaslian dokumen dengan menerbitkan dokumen tersebut dalam bentuk aset digital pada jaringan publik Blockchain [2] [3] [4]. Aset digital ini kemudian menjadi referensi bagi yang berkepentingan untuk memverifikasi dokumen atau salinannya dengan menggunakan QR code atau aplikasi khusus [5]. Selain pembuktian keaslian dokumen, pelacakan juga dapat dilakukan. Sebagai contoh, sebuah aset digital ijazah tidak akan dipublikasi tanpa adanya aset digital KHS (Kartu Hasil Studi) yang diterbitkan pada semester-semester sebelumnya. Setiap individu yang berkepentingan dapat melacak keaslian dan validitas dokumen berdasarkan hal tersebut.

Setiap aset digital yang dipublikasikan dalam jaringan Blockchain dapat didapatkan dan dibaca oleh semua pihak. Hal ini menjadi masalah, terutama pada data atau informasi yang bersifat pribadi. UU PDP (Perlindungan Data Pribadi) [6] menyatakan bahwa data yang bersifat pribadi seperti data pribadi yang bersifat spesifik (Informasi Kesehatan, Biometrik, Genetika) dan data pribadi yang bersifat umum (Nama Lengkap, Jenis Kelamin, Agama) tidak boleh dipublikasikan dan harus dilindungi. Hal ini kontradiktif dengan sifat Blockchain yang terbuka [7].

ZKP (*Zero Proof Knowledge*) adalah sebuah konsep dalam kriptografi yang pada implementasinya memungkinkan seseorang untuk membuktikan kebenaran suatu pernyataan kepada pihak lain tanpa harus mengungkapkan informasi rahasia apa pun selain kebenaran pernyataan tersebut [8]. Dengan kata lain, pengirim dapat membuktikan kepada penerima bahwa pernyataan yang mereka buat benar tanpa mengungkapkan detail sebenarnya yang membuktikan kebenaran pernyataan tersebut [9]. Pengirim informasi (*prover*) mengirimkan informasi rahasia yang ingin diverifikasi ke *verifier* dengan bantuan *randomizer*. Informasi rahasia tersebut kemudian diubah menjadi suatu statement yang harus diverifikasi oleh *verifier*. Randomizer kemudian mengirimkan kunci rahasia yang hanya diketahui oleh prover dan verifier untuk memastikan kebenaran informasi yang diberikan oleh prover [10].

Dalam Blockchain, pemanfaatan ZKP dalam sistem verifikasi dokumen digital diprogram dalam bentuk Smart Contract.

Smart contract dirancang untuk mengeksekusi, menegosiasikan, dan memverifikasi kontrak secara otomatis tanpa adanya pihak ketiga. sehingga meminimalisir adanya kesalahan dan mempercepat proses verifikasi [11]. Smart contract juga memungkinkan proses verifikasi dilakukan secara transparan, karena setiap transaksi yang dilakukan dalam smart contract dapat diverifikasi oleh seluruh pengguna jaringan Blockchain.

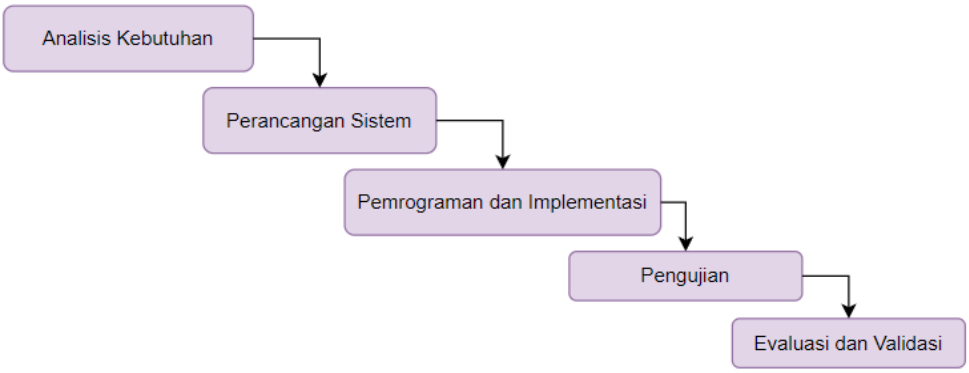
Dalam penelitian ini Smart Contract diimplementasikan dan dideploy pada jaringan Blockchain publik Polygon (MATIC). Penggunaan jaringan Polygon (MATIC) yang dibangun dengan protokol konsensus PoS (Proof of Stake) memungkinkan proses verifikasi dokumen yang lebih cepat, hemat biaya, dan dapat diakses secara luas oleh pengguna yang memerlukan verifikasi dokumen [12].

METODE PENELITIAN

Penelitian ini bertujuan untuk membangun sistem verifikasi dokumen digital berbasis Zero-Knowledge Proof (ZKP) dan teknologi Blockchain menggunakan metodologi pengembangan perangkat lunak System Development Life Cycle (SDLC). Metode penelitian ini terdiri dari beberapa fase perancangan dan pembangunan yang saling terkait seperti pada Gambar 1.

1. Analisis Kebutuhan

   Pada fase analisis kebutuhan, kami mengidentifikasi dan mendefinisikan secara rinci kebutuhan fungsional dan non-fungsional yang diperlukan untuk menerbitkan dan memverifikasi dokumen dalam lingkungan Blockchain menggunakan mekanisme ZKP. Kebutuhan fungsional mencakup fungsi-fungsi utama sistem seperti pembuatan dokumen, penerbitan dalam Blockchain, dan verifikasi dengan ZKP. Sementara itu, kebutuhan non-fungsional mencakup aspek-aspek seperti keamanan, kinerja, skalabilitas, dan interoperabilitas dengan sistem lain.



Gambar 1. Diagram Metode Penelitian

2. Perancangan Sistem

   Pada fase perancangan sistem, kami merinci arsitektur sistem secara menyeluruh. Algoritma yang akan diimplementasikan dalam Smart Contract dirancang dengan mendalam, termasuk proses penerbitan dokumen, integrasi ZKP, dan penyimpanan data dalam Blockchain. Selain itu, kami melakukan validasi terhadap desain algoritma ini untuk memastikan kesesuaian dengan tujuan dan kebutuhan sistem.

3. Pemrograman dan Implementasi

   Fase pemrograman dan implementasi melibatkan konversi desain algoritma ke dalam kode nyata pada Smart Contract. Proses ini mencakup pengembangan kode yang akurat dan efisien, memperhatikan prinsip keamanan dalam pengembangan kontrak pintar, serta mengintegrasikan mekanisme ZKP sesuai dengan spesifikasi yang telah ditetapkan.

4. Pengujian

   Pada tahap pengujian, kami melakukan serangkaian uji fungsionalitas dan kinerja terhadap Smart Contract yang telah diimplementasikan. Pengujian ini mencakup simulasi situasi nyata di mana Smart Contract dipanggil melalui berbagai metode seperti pemanggilan fungsi melalui wallet kripto atau program web3. Kami mengidentifikasi potensi cacat atau kelemahan dalam sistem, memastikan bahwa mekanisme ZKP berfungsi dengan benar, dan mengukur kinerja sistem dalam skenario berbeda.

5. Evaluasi dan Validasi

   Pada fase ini, hasil pengujian dianalisis secara mendalam untuk mengevaluasi kelayakan sistem. Kami memvalidasi bahwa sistem telah memenuhi tujuan awal dan kebutuhan yang ditetapkan, termasuk aspek keamanan, efisiensi, dan kemampuan beradaptasi dengan perubahan lingkungan. Jika diperlukan, kami melakukan perbaikan atau penyesuaian lebih lanjut untuk meningkatkan kinerja dan keandalan sistem.

Dengan pendekatan SDLC, penelitian ini memastikan bahwa setiap tahap pengembangan sistem dilakukan dengan teliti dan terstruktur, menghasilkan solusi yang dapat diandalkan dalam penerbitan dan verifikasi dokumen digital menggunakan ZKP dan teknologi Blockchain.

HASIL PENELITIAN

Pendekatan awal dalam penelitian ini melibatkan identifikasi secara komprehensif terhadap kebutuhan fungsional dan non-fungsional yang esensial dalam sistem verifikasi dokumen. Kebutuhan ini selanjutnya diimplementasikan dalam bentuk Smart

Contract yang memadukan konsep Zero-Knowledge Proof (ZKP) dengan teknologi Blockchain.

Kebutuhan fungsional, yang dinyatakan dalam poin FR1 hingga FR4, telah dikonsolidasikan dan dipresentasikan dalam Tabel 1, sementara kebutuhan non-fungsional yang tercakup dalam poin NR1 hingga NR4, disajikan dalam Tabel 2 sebagai panduan fundamental dalam pengembangan sistem ini.

Tabel 1. Kebutuhan Fungsional

No	Nama	Keterangan
FR1	Sistem harus dapat memverifikasi keaslian dokumen secara cepat dan akurat.	Smart Contract akan menyimpan hash dari dokumen dan informasi verifikasi yang diperlukan.
FR2	Sistem harus dapat menampilkan riwayat verifikasi dokumen	Setiap kali verifikasi dilakukan, catatan tentang waktu, hasil verifikasi, dan identitas pihak yang melakukan verifikasi akan disimpan dalam Blockchain.
FR3	Sistem harus dapat menyimpan dokumen dan data pengguna dengan aman dan terenkripsi.	Smart Contract menggunakan fitur enkripsi yang disediakan oleh protokol Ethereum atau mekanisme enkripsi khusus untuk memastikan keamanan dan privasi dokumen serta data pengguna yang disimpan di dalamnya.
FR4	Sistem harus dapat mengirimkan notifikasi verifikasi dokumen kepada pengguna.	Smart Contract dapat memicu notifikasi kepada pengguna melalui transaksi blockchain atau memicu tindakan lain yang mengirimkan pemberitahuan ke aplikasi atau layanan eksternal yang terkait dengan pengguna
FR4	Sistem harus dapat menghubungkan pengguna dengan pihak yang membutuhkan verifikasi dokumen.	Smart Contract dapat memfasilitasi pertukaran bukti verifikasi ZKP antara pengguna yang memiliki dokumen yang perlu diverifikasi dan pihak atau organisasi yang memerlukan verifikasi.

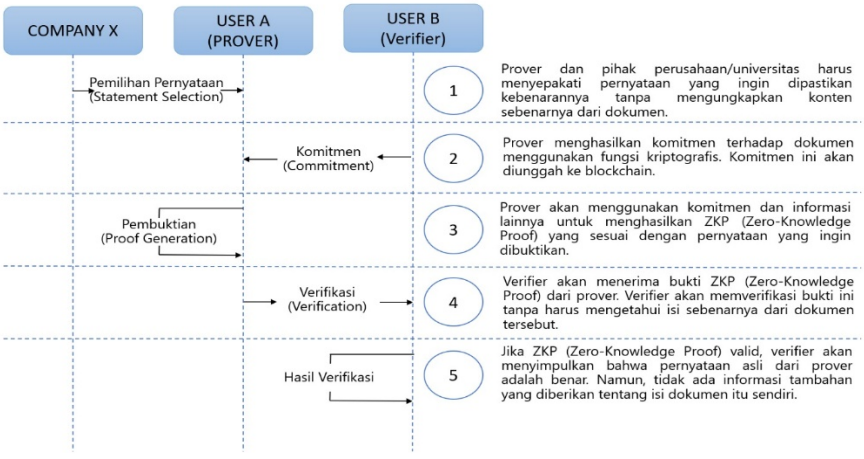
Tabel 2. Kebutuhan Non-Fungsional

No	Nama	Keterangan
NR1	Sistem harus memiliki performa yang cepat dan responsif	Polygon memiliki skalabilitas dan biaya transaksi yang rendah. Selain itu, desain Smart Contract yang dioptimalkan agar eksekusi kontrak lebih efisien dan tidak memakan waktu yang lama
NR2	Sistem harus mudah diakses dan digunakan oleh pengguna.	Pengguna diberikan petunjuk jelas dan langkah-langkah yang mudah diikuti untuk melakukan verifikasi dokumen menggunakan ZKP
NR3	Sistem harus memiliki tingkat keamanan yang tinggi untuk melindungi dokumen dan data pengguna.	Mekanisme enkripsi untuk menyimpan data secara aman, validasi yang tepat untuk memastikan keaslian verifikasi ZKP, dan pengaturan izin akses yang tepat untuk mencegah akses yang tidak sah ke Smart Contract.
NR4	Sistem harus terus diperbarui dan dioptimalkan untuk meningkatkan kinerjanya.	Tim pengembang akan selalu memantau dan menganalisis kinerja sistem untuk mengidentifikasi area yang memerlukan perbaikan.

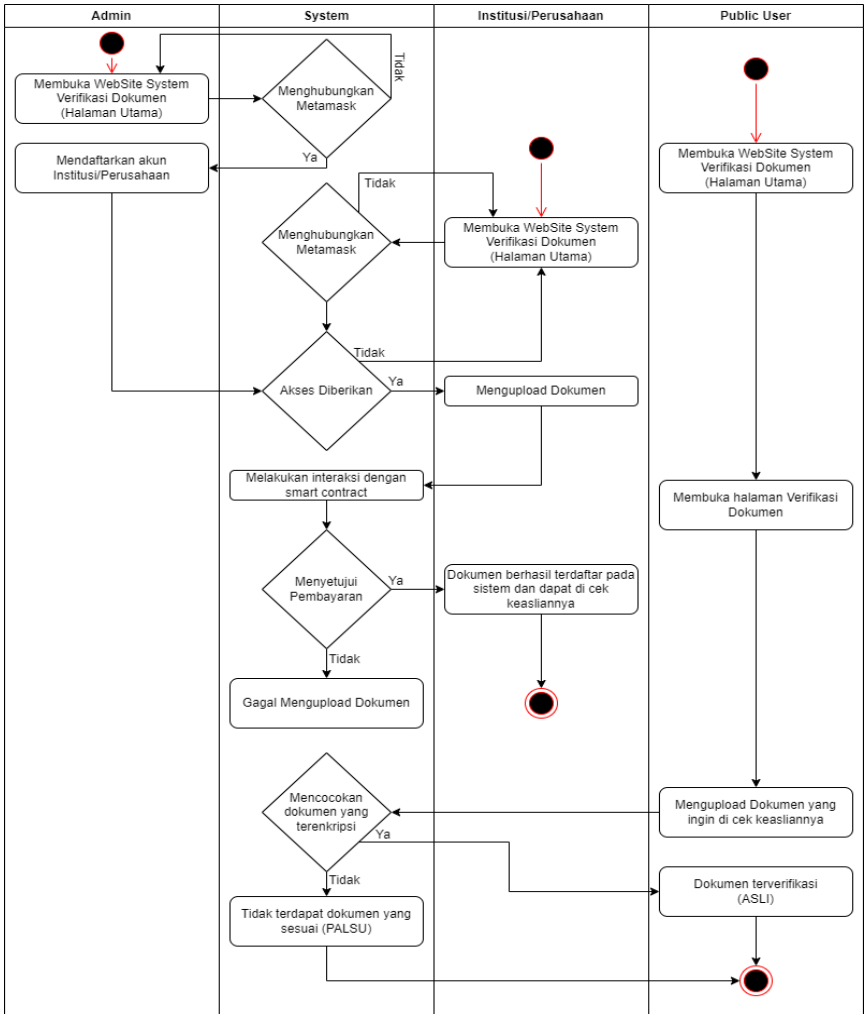
Setelah kebutuhan fungsional telah teridentifikasi, berikutnya adalah merancang mekanisme verifikasi dengan ZKP. Gambar 2 menggambarkan diagram interaksi antara pihak yang berkepentingan dalam proses verifikasi dokumen. Terdapat tiga entitas yang berinteraksi dalam sistem ini, penerbit document (Company X), pemilik dokumen (prover), dan pihak ketiga yang akan memverifikasi keaslian dokumen (verifier). Pertama, penerbit dokumen menyepakati informasi mana yang akan dibuat untuk publik dan mana yang bersifat pribadi atau privat, dan mengunggah dokumen yang berisi informasi publik ke Blokchain. Verifier memberikan komitmen kepada prover tentang data privat yang akan diverifikasi (misalnya nilai dalam ijazah) dengan menggunakan fungsi kriptografis [13]. Prover kemudian mengkalkulasi sebuah "*proof*" atau bukti sesuai dengan pernyataan atau data mengenai Prover yang akan dibuktikan di dalam dokumen. Verifier yang mendapatkan *proof* tersebut akan melakukan kalkulasi terhadap *proof* untuk mendapatkan informasi keabsahan data privat tanpa mengungkap data privat tersebut [14].

Dengan menggunakan dasar verifikasi ZKP, perancangan sistem secara keseluruhan digambarkan pada Gambar 3. Pada sistem ini, Admin memiliki peran penting sebagai inisiator dan pengatur akses ke wallet yang digunakan oleh institusi atau perusahaan. Admin dapat melakukan login ke dalam sistem menggunakan wallet admin yang kemudian memberikan akses ke pengguna (prover) dan pemeriksa dokumen (verifier).

Setelah akses diberikan, institusi atau perusahaan dapat menggunakan sistem dengan mengupload dokumen- yang ingin diverifikasi ke dalam sistem Blockchain melalui Smart Contract. Setelah dokumen terunggah, sistem akan memproses verifikasi keabsahan dokumen dengan menggunakan ZKP. Penerbit dokumen akan menyepakati informasi yang bersifat publik dan pribadi, lalu mengunggah dokumen dengan informasi publik ke dalam Blockchain.



Gambar 2. Diagram Interaksi Proses Verifikasi Dokumen Berbasis ZKP



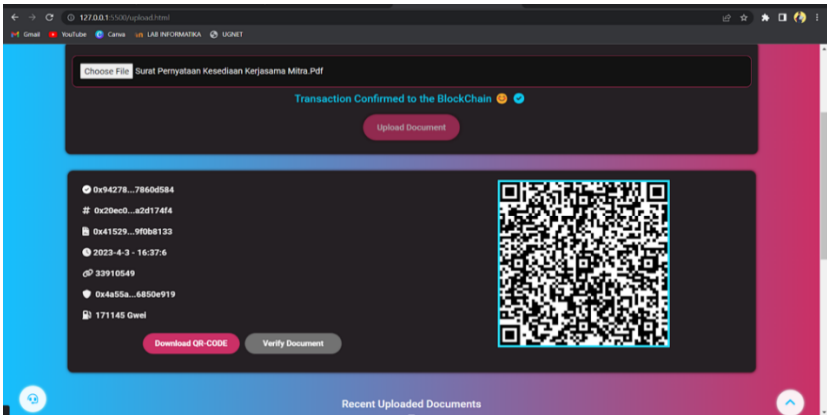
Gambar 3. Diagram Aktivitas Sistem Verifikasi Dokumen

HASIL DAN PEMBAHASAN

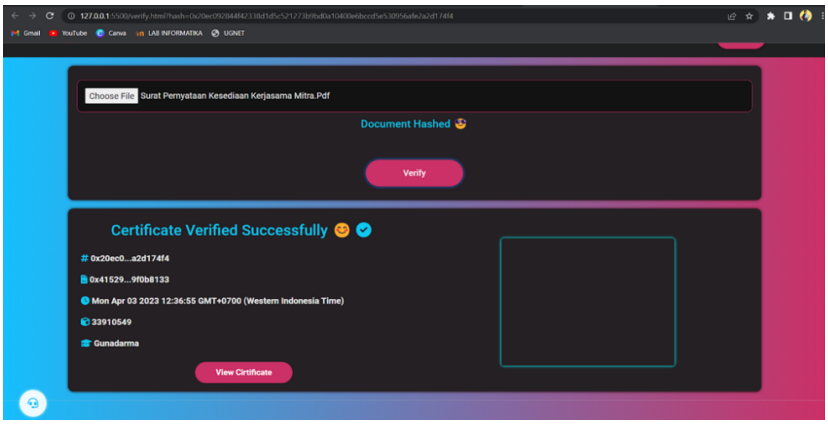
Pemanfaatan Zero-Knowledge Proof (ZKP) dalam kerangka sistem verifikasi dokumen berbasis teknologi Blockchain membawa dampak signifikan terhadap perlindungan privasi dan keamanan dokumen, tanpa mengesampingkan integritas proses verifikasi itu sendiri. Proses inovatif ini memberikan kemampuan bagi para pengguna untuk memverifikasi suatu pernyataan dengan mempertahankan kerahasiaan informasi yang sensitif dan pribadi, tanpa harus mengungkapkan rincian detail yang berisiko [15]. Smart Contract yang berhasil dikembangkan selanjutnya diintegrasikan dengan jaringan Blockchain Polygon, mendorong eksplorasi potensi kemajuan dalam skalabilitas dan efisiensi transaksi. Ditambah dengan antarmuka aplikasi berbasis Web3, pengguna diberikan kesempatan untuk berinteraksi langsung dengan Smart Contract ini. Ilustrasi visual pada Gambar 4 dan Gambar 5 memvisualisasikan dengan jelas bagaimana antarmuka pengguna memungkinkan interaksi yang lancar dengan Smart Contract melalui aplikasi Web3 yang disediakan. Dengan demikian, penggunaan sistem ini

menghasilkan dampak yang kuat dalam merampingkan proses verifikasi dokumen tanpa mengorbankan aspek privasi dan keamanan yang esensial.

Hasil pengujian fungsional sistem secara keseluruhan terdapat pada Tabel 3 yang merangkum hasil uji fungsionalitas sistem secara komprehensif. Uji fungsional (FR1), yang melibatkan proses unggah dokumen melalui antarmuka Web3 ke jaringan Blockchain, menghasilkan nilai hash unik dari dokumen yang kemudian dicatat dalam Smart Contract. Melalui fitur penjelajahan Blockchain serta antarmuka Web3 yang tersedia, pengguna dapat dengan mudah mengakses dan melacak sejarah unggah serta verifikasi dokumen (FR2). Kelebihan dari teknologi Blockchain adalah kemampuannya untuk merekam setiap transaksi dengan keamanan tinggi, memastikan integritas dan ketidakmampuan untuk mengubah atau menghapus transaksi, termasuk unggahan dan verifikasi dokumen yang tercatat dalam Blockchain.



Gambar 4. Tampilan Unggah Dokumen Ke Blockchain



Gambar 5. Tampilan Hasil Verifikasi Dokumen

Tabel 3. Hasil Pengujian Smart Contract Sistem Verifikasi Dokumen

No	Nama	Output Yang Diharapkan	Keterangan	HASIL
FR1	Sistem harus dapat memverifikasi keaslian dokumen secara cepat dan akurat.	Sistem dapat memveri- fikasi dokumen.	Saat dokumen di upload sistem akan langsung memeriksa hash dokumen tanpa melihat isi dari dokumen tersebut.	Sukses
FR2	Sistem harus dapat menampilkan riwayat verifikasi dokumen	Sistem manampilkan ri- wayat verifikasi doku- men	Riwayat verifikasi tersimpan dalam hash unik pada setiap dokumen yang apabila diakses ulang akan menampilkan data waktu kapan dokumen tersebut terdaftar pada sistem.	Sukses
FR3	Sistem harus dapat menyimpan dokumen dan data pengguna dengan aman dan terenkripsi.	Dokumen disimpan da- lam bentuk hash	Sebelum mendapatkan hash dokumen terlebih dahulu dienkripsi oleh protokol ethereum.	Sukses
FR4	Sistem harus dapat mengirimkan notifikasi verifikasi dokumen kepada pengguna.	Muncul notifikasi saat dokumen berhasil dive- rifikasi.	Sistem memberitahu bahwa dokumen yang diverifikasi masih asli atau sudah di-edit (palsu)	Sukses
FR5	Sistem harus dapat menghubungkan pengguna dengan pihak yang membutuhkan verifikasi dokumen.	Terdapat tiga sisi antarmuka untuk client (perusahaan/universitas), pengguna(verifier), pengembang (profer)	Ketiga antarmuka dapat diakses dan memiliki role/fungsi nya masing-masing.	Sukses

Smart Contract yang dirancang menggunakan event handler untuk melakukan notifikasi kepada pengguna (FR4) jika verifikasi dokumen berhasil (Gambar 10). Pengguna secara visual dapat melakukan konfirmasi terhadap verifikasi ini. Selain itu, tiga antar muka yang dibangun untuk prover, verifier, randomizer merupakan penghubung antara pemangku kepentingan dalam sistem verifikasi dokumen dengan menggunakan Blockchain. Melalui pengujian ini, fungsi Smart Contract dengan menggunakan antar muka Web3 telah memenuhi semua kebutuhan fungsionalitas yang telah didefinisikan sebelumnya. Untuk mengetahui persepsi pengguna sistem terhadap fungsi dari sistem yang telah dibangun, dilakukan survei terhadap 52 responden yang merupakan pengguna sistem. Dalam evaluasi fungsionalitas sistem, pengguna diberi kesempatan untuk memberikan tanggapan atas beberapa pertanyaan kunci terkait fungsi dan kinerja sistem. Fokus survei adalah pada kinerja sistem dalam menghadapi beban pengguna yang tinggi dan kemampuan sistem untuk menjaga kualitas waktu konfirmasi transaksi serta biaya transaksi yang terjangkau. Melalui survei ini, tanggapan pengguna memberikan wawasan berharga mengenai kinerja dan kehandalan sistem, serta

kemampuannya dalam memenuhi harapan dan kebutuhan pengguna secara efisien. Tabel 4 mengetengahkan hasil survei tersebut. Keseluruhan pengguna menyatakan bahwa sistem telah berfungsi seperti yang diharapkan. Bahwa sistem dapat menangani format dokumen berbeda dan dapat memverifikasi integritas atau validitas dokumen. Pengguna juga menyatakan bahwa sistem dapat menangani beban tinggi, cepat dan tetap stabil. Penggunaan Blockchain Polygon yang berbiaya transaksi rendah juga dianggap suatu kelebihan untuk keberlanjutan penggunaan sistem.

Tabel 4. Hasil Survei

EVALUASI FUNGSIONALITAS SISTEM		
Pertanyaan	**Jawaban @User**	
	Ya	**Tidak**
Apakah pengguna dapat mengunggah dokumen dengan format yang berbeda-beda.	52	0
Apakah sistem dapat memvalidasi dokumen yang diunggah oleh pengguna dengan menggunakan algoritma hash dan menyimpan hash dokumen tersebut di blockchain.	52	0
Apakah sistem dapat menampilkan status validasi dokumen dengan jelas untuk pengguna, seperti valid atau tidak valid.	52	0
EVALUASI EFEKTIFITAS SISTEM		
Pertanyaan	**Jawaban @User**	
	Ya	**Tidak**
Apakah sistem dapat menangani beban pengguna yang tinggi dan tetap berjalan stabil tanpa menurunkan performa.	52	0
Apakah waktu konfirmasi transaksi dalam sistem dapat diperta- hankan sesuai dengan kebutuhan, seperti waktu konfirmasi transaksi yang cepat.	52	0
Apakah biaya transaksi dalam sistem dapat dipertahankan rendah dan terjangkau untuk pengguna.	52	0

PENUTUP

Dalam penelitian ini smart contract berhasil dirancang dan dikembangkan sebagai bagian dari sistem verifikasi dokumen berbasis teknologi blockchain yang diterapkan pada jaringan Polygon (MATIC). Penerapan sistem verifikasi dokumen yang mengadopsi konsep Zero Knowledge Proof (ZKP) berhasil meningkatkan tingkat keamanan dan privasi dalam proses verifikasi dokumen. Penggunaan jaringan MATIC sebagai infrastruktur telah membawa manfaat signifikan, termasuk waktu transaksi yang lebih cepat dan biaya yang relatif rendah dibandingkan jaringan Blockchain lainnya. Implementasi sistem verifikasi dokumen berbasis blockchain dengan pendekatan ZKP pada jaringan MATIC meningkatkan kepercayaan dalam proses verifikasi dokumen. Melalui pengembangan lebih lanjut, sistem ini memiliki potensi untuk diintegrasikan dengan sistem manajemen dokumen perusahaan, memperkuat efisiensi dan efektivitas proses verifikasi secara keseluruhan.

Di samping itu, perlu dilakukan upaya untuk mengedukasi calon pengguna tentang teknologi Blockchain dan pengoperasian Blockchain wallet dalam menggunakan sistem. Selain itu, aspek hukum dan regulasi terkait penerapan sistem verifikasi dokumen berbasis blockchain dengan ZKP di Indonesia juga perlu mendapatkan perhatian lebih lanjut melalui penelitian yang komprehensif. Penelitian ini menjadi pijakan penting dalam menggali potensi teknologi blockchain dalam memajukan proses verifikasi dokumen, dan pelbagai langkah masa depan perlu diambil guna mewujudkan manfaat maksimal dari inovasi ini dalam dunia praktis dan kebijakan.

DAFTAR PUSTAKA

[1] Republik Indonesia, *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK,* Jakarta, 2016.

[2] G. Sethia, S. Namratha, H. Srikanth and S. Sreeja C, "Academic Certificate Validation Using Blockchain Technology," Pune, 2022.

[3] M. Effiong, A. Norta, C. Udokwu and M. Hattingh, "Adoption of Blockchain Technology in Academic Certificate-Verification Systems," Irvine, 2022.

[4] T. Nurhaeni, I. Handayani, F. Budiarty, D. Apriani and P. A. Sunarya, "Adoption of Upcoming Blockchain Revolution in Higher Education: Its Potential in Validating Certificates," Gorontalo, 2020.

[5] M. A. Kusuma, P. Sukarno and A. A. Wardana, "Security System for Digital Land Certificate Based on Blockchain and QR Code Validation in Indonesia," Bandung, 2022.

[6] Republik Indonesia, *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI,* 2022.

[7] Z. Wang, J. Lin, Q. Cai, Q. Wang, D. Zha and J. Jing, "Blockchain-Based Certificate Transparency and Revocation Transparency," *IEEE Transactions on Dependable and Secure Computing,* vol. 19, no. 1, p. 681–697, 2022.

[8] D. Hou, J. Zhang, S. Huang, Z. Peng, J. Ma and X. Zhu, "Privacy-Preserving Energy Trading Using Blockchain and Zero Knowledge Proof," Espoo, 2022.

[9] D. Čapko, S. Vukmirović and N. Nedić, "State of the Art of Zero-Knowledge Proofs in Blockchain," Belgrade, 2022.

[10] S. Liu, "Privacy Protection Revolution: Zero-knowledge Proof," Zakopane, 2022.

[11] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari and Y. Cao, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access,* vol. 9, p. 61048–61073, 2021.

[12] L. Liu, J. Wan and W. Yue, "Computer Assisted Design of Intelligent E-Certificate System Based on Blockchain Technology," Zakopane, 2022.

[13] S. Almuhammadi and C. Neuman, "Security and privacy using one-round zero-knowledge proofs," Munich, 2005.

[14] M. K. Ibrahem, "Modification of Diffie-Hellman key exchange algorithm for Zero knowledge proof," Baghdad, 2012.

[15] L. Cao and Z. Wan, "Anonymous scheme for blockchain atomic swap based on zero-knowledge proof," Dalian, 2020.