Jurnal SimanteC
Vol. 14, No. 1 Desember 2025
P-ISSN : 2088-2130
E-ISSN : 2502-4884

Penerapan teknologi *blockchain* berbasis *smart contract* untuk meningkatkan keamanan transaksi finansial online

Application of smart contract-based blockchain technology to improve the security of online financial transactions

[1]Steven Aprianto Wirayuda*, [2] Siti Lailiyah, [3]Ahmad Fajri

[1,2,3]Teknik Infomatika, STMIK Widya Cipta Dharma
Jl.M.Yamin No.25, Gn. Kelua, Kec. Samarinda Ulu, Kota Samarinda, Kalimantan Timur 75123, Indonesia
*e-mail: [1]2143040@wicida.ac.id, [2]lai.59a@gmail.com,[3]ahmadfajri@wicida.ac.id

Abstrak

Transformasi digital dalam sektor keuangan menuntut adanya sistem transaksi yang tidak hanya cepat dan efisien, tetapi juga aman dan transparan. Penelitian ini membahas penerapan teknologi blockchain sebagai solusi terhadap permasalahan pada sistem transaksi finansial online yang masih bergantung pada sistem terpusat dan rentan terhadap manipulasi. Tujuan dari penelitian ini adalah merancang arsitektur sistem keamanan transaksi finansial berbasis blockchain yang dapat diuji melalui pendekatan simulasi konseptual. Penelitian menggunakan pendekatan deskriptif kualitatif dengan alat bantu Ganache, MetaMask, dan Remix IDE dalam mensimulasikan transaksi menggunakan smart contract di lingkungan blockchain lokal. Kebaruan dari penelitian ini terletak pada penggabungan pemodelan sistem keamanan berbasis blockchain dengan pendekatan simulasi skenario realistis, yang belum banyak dibahas dalam studi sebelumnya. Kontribusi penelitian ini adalah menghasilkan model arsitektur modular yang menyusun komponen utama seperti pengguna, smart contract, validator, dan regulator dalam satu alur kerja terintegrasi yang dapat diadopsi untuk platform keuangan digital. Hasil simulasi menunjukkan bahwa sistem yang dibangun mampu meningkatkan keamanan, mempercepat validasi transaksi, memperkuat auditabilitas, dan mengurangi biaya operasional jika dibandingkan dengan sistem transaksi konvensional. Penelitian ini memberikan dasar yang kuat untuk pengembangan sistem finansial berbasis blockchain yang lebih luas dan tahan terhadap serangan eksternal.

Kata kunci: *Arsitektur Sistem, Blockchain, Keamanan Transaksi, Smart Contract, Simulasi*

Abstract

The digital transformation in the financial sector demands a transaction system that is not only fast and efficient but also secure and transparent. This study explores the application of blockchain technology as a solution to the problems found in centralized online financial transaction systems that are vulnerable to manipulation. The objective of this research is to design a blockchain-based financial transaction security system architecture that can be evaluated through a conceptual simulation approach. This study uses a descriptive qualitative method with tools such as Ganache, MetaMask, and Remix IDE to simulate smart contract-based transactions within a local blockchain environment. The novelty of this research lies in the integration of a security system modeling approach with realistic scenario-based simulations, which is rarely discussed in previous studies. The research contributes by producing a modular system architecture that integrates key components—users, smart contracts, validators, and regulators—into a cohesive workflow applicable to various digital financial platforms. Simulation results show that the proposed system enhances security, accelerates transaction validation, strengthens auditability, and reduces operational costs compared to conventional transaction systems. This

study provides a strong foundation for the broader development of blockchain-based financial systems that are more resistant to external attacks.

Keywords: *System Architecture, Blockchain, Transaction Security, Smart Contract, Simulation*

1 PENDAHULUAN

Transformasi digital telah membawa perubahan besar dalam suatu negara di berbagai sektor, salah satunya adalah industri finansial. Transaksi keuangan yang sebelumnya dilakukan secara manual kini telah beralih ke sistem *online* yang menawarkan kecepatan, kemudahan, efesiensi dan aksesibilitas yang tinggi [1].

Sistem transaksi finansial konvensional umumnya masih bergantung pada sistem yang masih mudah di serang *cyber*, yang menjadikan satu titik perhatian dalam segi keamanan, integritas data, serta potensi penyalahgunaan sistem, pencurian identitas, dan manipulasi transaksi menjadi ancaman nyata dalam *ekosistem digital* yang semakin kompleks [2]. Ketika sistem pusat terganggu atau disusupi, seluruh jaringan transaksi berisiko lumpuh. Kondisi ini memunculkan kebutuhan pendekatan baru dalam membangun sistem yang lebih aman, transparan, dan andal [3].

Fenomena dari transaksi finansial konvensional tersebut telah menerbitkan metode baru yaitu tentang teknologi *blockchain* yang hadir sebagai salah satu solusi potensial untuk menjawab tantangan tersebut. *Blockchain* merupakan teknologi penyimpanan data digital yang bersifat terdesentralisasi, di mana setiap transaksi tercatat dalam *blok* yang saling terhubung dan diamankan melalui kriptografi, sehingga menciptakan sistem yang transparan dan sulit dimanipulas [4],[5].Dengan prinsip desentralisasi, setiap transaksi dicatat dalam *blok* yang terdistribusi secara merata di seluruh jaringan, membuatnya lebih tahan terhadap manipulasi maupun serangan eksternal [6]. Selain itu, keunggulan *blockchain* dalam hal transparansi, auditabilitas, dan integritas data memberikan nilai tambah yang signifikan untuk penerapan dalam sistem finansial modern [7].

Di era digital ini dibutuhkannya pembaruan tentang keamanan atas transaksi finansial konvensional yang menjadi urgensi dari penelitian ini terletak pada meningkatnya kebutuhan sistem keamanan transaksi finansial *online* yang tidak hanya efektif dari sisi teknis, tetapi juga efisien, dapat diaudit secara real-time, serta mampu membangun kepercayaan pengguna dalam jangka panjang. Penerapan *blockchain* dalam konteks ini dinilai relevan dan strategis, terutama dalam upaya mengurangi ketergantungan pada sistem terpusat yang rentan terhadap celah keamanan.

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah bagaimana merancang sebuah arsitektur sistem yang mampu mendukung keamanan transaksi finansial *online* dengan mengadopsi teknologi *blockchain* dan bagaimana hasil dari simulasi sistem tersebut dapat menunjukkan keunggulan dalam hal keamanan dan efisiensi dibandingkan dengan sistem transaksi konvensional yang tidak berbasis *blockchain*. Melalui simulasi ini, efektivitas implementasi *blockchain* dapat diuji secara langsung dalam konteks perlindungan data, kecepatan transaksi, serta potensi pengurangan ketergantungan terhadap pihak ketiga [8].

Adapun tujuan dari penelitian ini adalah merancang sebuah model arsitektur sistem keamanan transaksi finansial berbasis teknologi *blockchain* yang dapat diuji secara konseptual dan analisis. Penelitian ini tidak berfokus pada pembangunan aplikasi secara langsung, melainkan pada pengembangan model dan simulasi berdasarkan skenario realistis dari *platform* keuangan *digital*. Dengan pendekatan ini, efektivitas dan validitas sistem dapat dianalisis tanpa harus melalui tahap implementasi penuh.

Kontribusi utama dari penelitian ini adalah pengembangan model arsitektur sistem keamanan transaksi finansial berbasis *blockchain* yang bersifat modular dan konseptual, yang belum banyak dibahas dalam studi sebelumnya. Penelitian ini juga menawarkan pendekatan simulatif menggunakan *Ganache*, *MetaMask*, dan Remix IDE sebagai metode evaluasi teknis terhadap performa *smart contract* dalam konteks transaksi digital. Selain itu, model yang dihasilkan memperjelas integrasi peran pengguna, *smart contract*, *validator*, dan *regulator* dalam satu alur kerja sistem, yang dapat dijadikan referensi bagi pengembang dan peneliti dalam merancang sistem keuangan digital yang lebih aman, efisien, dan dapat diaudit.

2 TINJAUAN PUSTAKA

Penelitian tentang penerapan teknologi blockchain dalam sistem keamanan transaksi finansial telah menunjukkan perkembangan yang pesat dalam lima tahun terakhir. penelitian [9] dan [10] sama-sama menyoroti pentingnya ledger terdistribusi, smart contract, serta sistem identitas digital dalam membangun sistem keuangan yang aman. Namun, kedua studi ini masih terbatas pada analisis teknis dan belum menawarkan model arsitektur modular yang fleksibel untuk diadopsi lintas platform finansial digital.

Upaya untuk memasukkan aspek privasi dan regulasi dalam desain arsitektur *blockchain* dilakukan penelitian [11], yang menekankan keseimbangan antara kebutuhan privasi pengguna dan kepatuhan terhadap regulasi. Sayangnya, penelitian ini tidak menjelaskan secara rinci bagaimana komponen kunci seperti validator dan regulator dapat disusun dalam satu arsitektur sistem yang sistematis. Sementara itu, penelitian [12] menggarisbawahi kebutuhan desain transaksi baru guna meminimalkan fraud di lingkungan keuangan, namun masih luput dalam menghadirkan solusi desain menyeluruh yang bersifat modular dan dapat direplikasi secara luas.

Penelitian [13] turut mengungkapkan potensi blockchain dalam memperkuat transparansi dan keamanan transaksi finansial. Namun, kajian ini lebih menekankan manfaat teoretis ketimbang penyusunan kerangka arsitektur sistem yang terintegrasi.

Berdasarkan pemetaan tersebut, dapat disimpulkan bahwa mayoritas studi sebelumnya masih berfokus pada aspek teoretis atau komponen tertentu secara terpisah (*ledger, smart contract*, atau regulasi), tanpa merancang arsitektur sistem keamanan finansial berbasis *blockchain* yang menyeluruh, terintegrasi, serta dapat diuji secara langsung melalui simulasi berbasis *smart contract*.

Penelitian ini menawarkan kebaruan melalui perancangan model arsitektur konseptual yang modular dan realistis, yang mencakup empat elemen utama pengguna, *smart contract*, *validator*, dan *regulator* dalam satu alur kerja terstruktur dan teruji melalui simulasi menggunakan Ganache, MetaMask, dan *Remix* IDE. Simulasi ini memungkinkan evaluasi praktis atas keamanan, efisiensi, auditabilitas, serta pengurangan biaya operasional dibandingkan sistem konvensional, suatu pendekatan yang belum dijelaskan secara eksplisit pada studi-studi sebelumnya. Berikut adalah hasil fokus perbandingan yang dapat dilihat pada Tabel 1.

Tabel 1. Perbandingan Penelitian

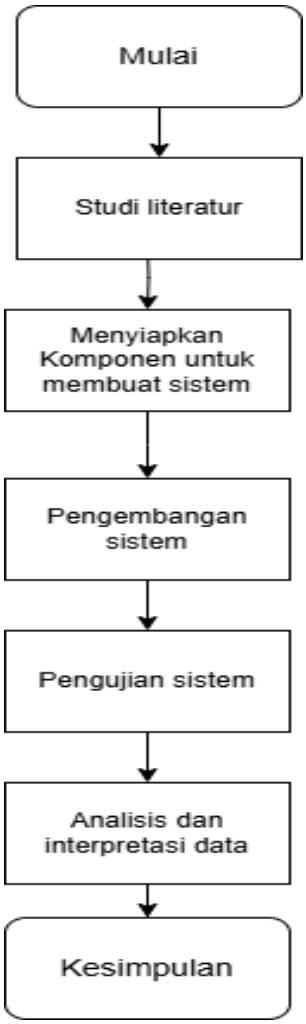
Author	Arsitektur	Komponen	Hasil simulasi
[9]	-	√	-
[10]	√	-	-
[11]	√	-	-
[12]	-	√	-
[13]	-	√	-
Author	√	√	√

Berbeda dari studi-studi sebelumnya yang masih terfokus pada aspek teoritis atau komponen tunggal sistem, penelitian ini diarahkan untuk menghasilkan prototipe arsitektur yang dapat diuji secara langsung melalui simulasi, sehingga memberikan gambaran konkret tentang bagaimana integrasi komponen pengguna, *smart contract*, validator, dan regulator dapat dioperasikan dalam satu kesatuan sistem yang fungsional. Model ini diharapkan tidak hanya melengkapi kekurangan dalam literatur, tetapi juga memberikan kerangka aplikatif yang dapat menjadi referensi bagi pengembangan sistem keuangan digital berbasis blockchain di masa depan.

3 METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif karena tujuan utamanya adalah untuk menggali secara mendalam konsep, proses, dan perancangan arsitektur sistem keamanan transaksi finansial berbasis *blockchain*, bukan untuk menguji hipotesis atau hubungan variabel secara kuantitatif. Pendekatan ini memungkinkan peneliti untuk memahami secara kontekstual bagaimana komponen-komponen utama seperti pengguna, *smart contract, validator,* dan

regulator berinteraksi dalam sistem *blockchain* yang dirancang melalui pengamatan proses simulasi dan dokumentasi sistem. Diagram alur penelitian dapat dilihat pada gambar 1.



Gambar 1. Diagram alur penelitian

Pendekatan deskriptif kualitatif sangat sesuai untuk penelitian yang bertujuan menggambarkan fenomena kompleks atau sistem teknologi tertentu secara utuh dalam konteks aslinya, khususnya pada objek kajian yang belum banyak dieksplorasi secara empiris [14]. Pendekatan ini juga cocok digunakan dalam penelitian yang mengembangkan model atau kerangka kerja baru seperti desain arsitektur blockchain yang masih dalam tahap konseptualisasi [15]. Dengan demikian, pendekatan ini relevan untuk mendukung pengembangan model arsitektur sistem keamanan *blockchain* yang teruji melalui simulasi, tanpa harus bergantung pada pengumpulan data numerik atau eksperimen kuantitatif.

Teknik pengumpulan data dilakukan melalui tiga metode utama, yaitu studi literatur, dokumentasi sistem, dan observasi hasil simulasi menggunakan *Ganache, MetaMask*, dan *Remix* IDE. Studi literatur digunakan untuk memperoleh landasan teoritis mengenai penerapan teknologi blockchain dalam sistem keuangan, sedangkan dokumentasi sistem mencatat setiap konfigurasi dan implementasi *smart contract* selama proses simulasi. Observasi dilakukan untuk mencatat proses validasi transaksi, pembuatan blok, dan pencatatan kontrak dalam jaringan *blockchain* lokal. Kombinasi ketiga teknik ini dirancang untuk mengintegrasikan pemahaman teoretis dengan bukti empiris, sehingga dapat menggambarkan performa sistem secara utuh dalam lingkungan terkontrol. Penggunaan dokumentasi dan observasi dalam penelitian kualitatif sangat dianjurkan untuk memperkaya data dan memperoleh pemahaman kontekstual yang mendalam terhadap objek penelitian [15].

Data yang dikumpulkan dianalisis menggunakan analisis konten dan pemetaan struktural. Analisis konten bertujuan untuk menginterpretasikan data hasil observasi simulasi secara

sistematis, khususnya terkait proses validasi transaksi, pencatatan *smart contract,* serta pembentukan blok dalam *blockchain*. Sementara itu, pemetaan struktural digunakan untuk menggambarkan hubungan antar komponen utama arsitektur yaitu pengguna, *smart contract*, *validator*, dan *regulator* secara konseptual, sehingga memudahkan evaluasi integritas sistem.

4 HASIL DAN PEMBAHASAN

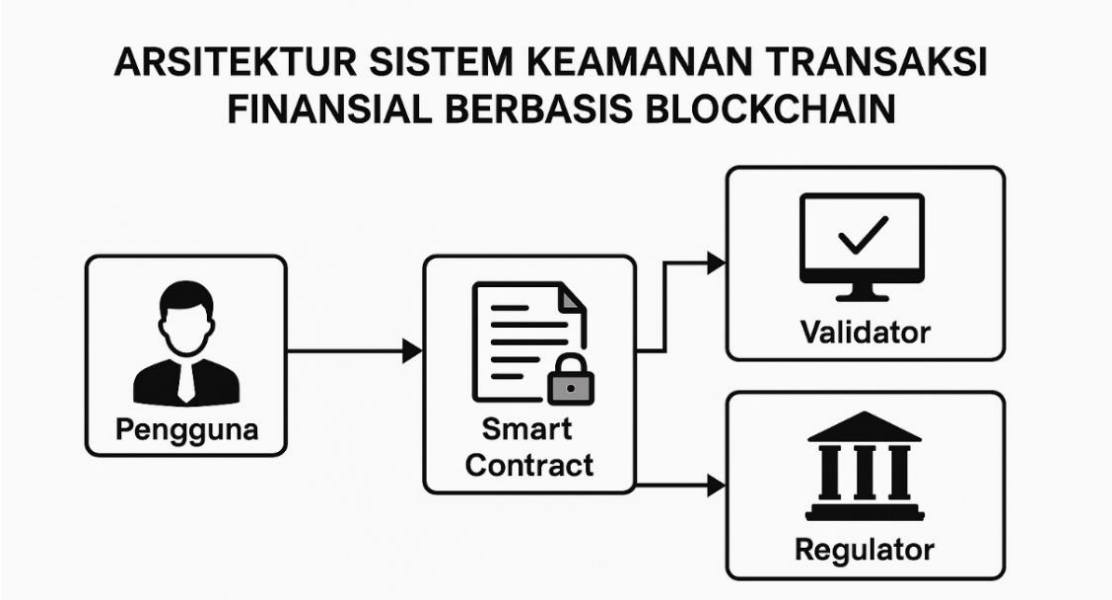
Hasil penelitian ini menyajikan rancangan arsitektur sistem keamanan transaksi finansial berbasis blockchain beserta hasil simulasi yang mendukung efektivitas model tersebut. Sebelum membahas lebih jauh mengenai komponen sistem, *deployment smart contract*, hingga validasi transaksi, bagian ini terlebih dahulu menguraikan gambaran umum rancangan dan simulasi yang dilakukan. Tujuannya adalah agar pembaca memperoleh pemahaman menyeluruh tentang ruang lingkup sistem yang diuji, alur pelaksanaan simulasi, serta konteks pengujian smart contract yang digunakan dalam penelitian ini.

a. Desain Arsitektur Sistem

Sistem keamanan transaksi finansial berbasis blockchain yang dikembangkan dalam penelitian ini terdiri dari empat komponen utama, yaitu pengguna (*user*), *smart contract*, *validator,* dan *regulator*. Masing-masing komponen memiliki peran spesifik yang saling terintegrasi dalam mendukung proses transaksi digital yang aman dan efisien. Pengguna berperan sebagai pihak yang menginisiasi dan melakukan transaksi dalam sistem. *Smart contract* bertugas menjalankan logika validasi dan pencatatan transaksi secara otomatis tanpa campur tangan pihak ketiga. *Validator* berfungsi untuk memverifikasi validitas transaksi berdasarkan kesepakatan jaringan *blockchain*, sehingga menjamin keamanan setiap proses transfer data atau aset. Sementara itu, *regulator* bertanggung jawab mengawasi kesesuaian transaksi dengan ketentuan dan regulasi yang berlaku, guna memastikan kepatuhan hukum dalam sistem. Keempat komponen ini dirancang untuk beroperasi secara sinergis, menciptakan arsitektur sistem yang tidak hanya terdesentralisasi dan aman, tetapi juga transparan serta dapat diaudit secara real-time, yaitu:

1) Penguna (*User*): menginisiasi transaksi *digital*
2) *Smart Contract:* Menangani logika validasi dan pencatatan transaksi
3) *Validator*: memastikan transaksi valid melalui konsensus jaringan
4) *Regulator*: mengawasi kepatuhan

Berikut adalah desain arsitektur sistem yang telah dibuat yang dapat dilihat pada gambar 2.



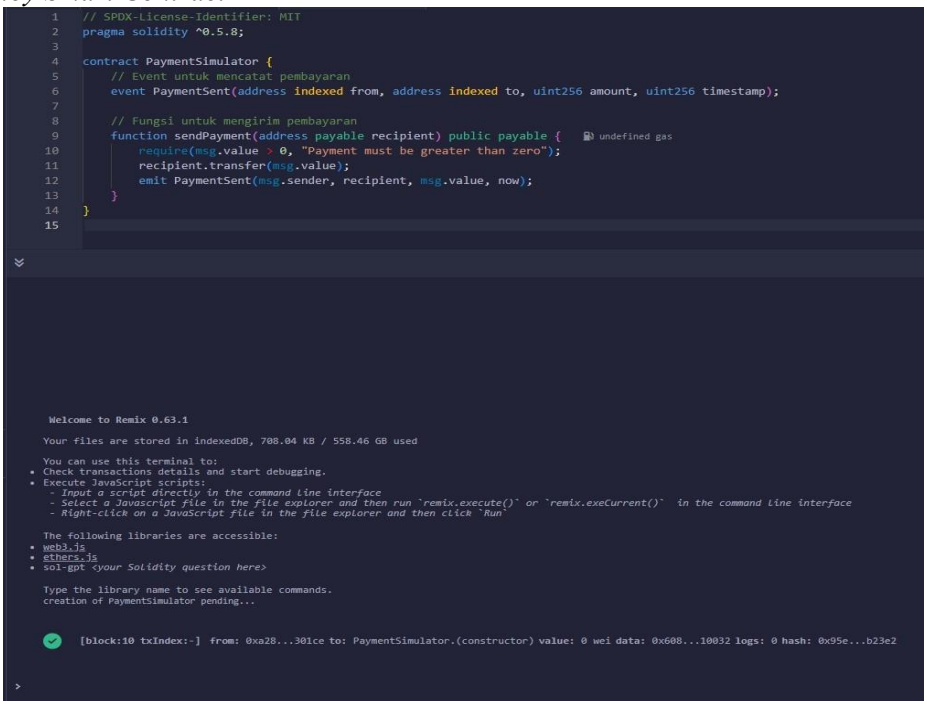
Gambar 2. Arsitektur Sistem Keamanan Transaksi Finansial Berbasis *Blockchain*

b. Simulasi

Simulasi dalam penelitian ini dilaksanakan dengan memanfaatkan beberapa perangkat utama berbasis *Ethereum*. *Ganache* digunakan sebagai jaringan *blockchain* lokal yang memungkinkan

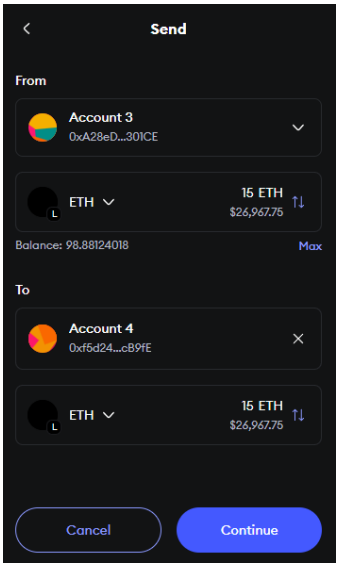
pengujian transaksi secara privat dan efisien. *MetaMask* berfungsi sebagai dompet *digital* yang menghubungkan pengguna dengan jaringan tersebut, memungkinkan pengelolaan akun serta pengiriman transaksi. Sementara itu, *Remix IDE* dimanfaatkan untuk menulis, mengompilasi, dan menerapkan *smart contract* berbasis *Solidity* ke jaringan lokal. Kombinasi ketiga alat ini mendukung pengujian menyeluruh terhadap proses transaksi yang aman dan otomatis menggunakan teknologi *blockchain*.

c. Deploy Smart Contract



Gambar 3. *Deploy Smart Contarct* di Remix IDE

Gambar 3 menunjukkan tahapan proses *deployment smart contract PaymentSimulator* yang dikembangkan menggunakan bahasa pemrograman *Solidity* versi ^0.5.8 di platform Remix IDE. *Smart contract* ini dirancang untuk mengelola pengiriman ETH antar akun serta mencatat setiap transaksi yang terjadi melalui *event* bernama *PaymentSent*, yang merekam data penting seperti alamat pengirim, penerima, jumlah ETH yang dikirim, serta waktu transaksi. Fungsi utama dalam kontrak ini, yaitu *sendPayment,* dilengkapi dengan validasi nilai transfer guna memastikan bahwa hanya transaksi dengan jumlah yang valid yang dapat diproses dan dicatat ke dalam *blockchain.* Pada saat proses *deployment*, terminal Remix IDE menampilkan informasi detail terkait status *deployment smart contract,* termasuk data blok, alamat kontrak baru yang terbentuk, serta hash transaksi yang dihasilkan. Seluruh informasi ini menjadi bukti transparansi dan integritas dari setiap proses *deployment* yang berlangsung di lingkungan pengembangan lokal.

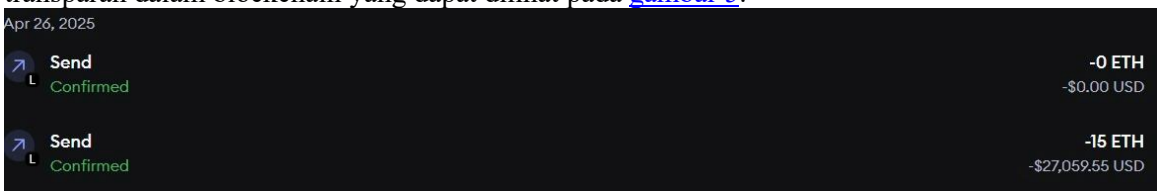


Gambar 4. Pengiriman sejumlah *ethereum* (ETH) di *Metamask*

Gambar 4 menampilkan proses pengiriman 15 e*thereum* (ETH) melalui *MetaMask* dari *Account* 3 (0xA28eD...301CE) ke *Account* 4 (0xf5d24...cB9FE), dengan nilai transaksi setara $26,967.75. Saldo awal pengirim tercatat 98.88 *ETH*. gambar menunjukkan detail aset, jumlah, dan alamat tujuan secara jelas sebelum pengguna menekan tombol "*Continue*" untuk melanjutkan transaksi.

d. Simulasi Transaksi

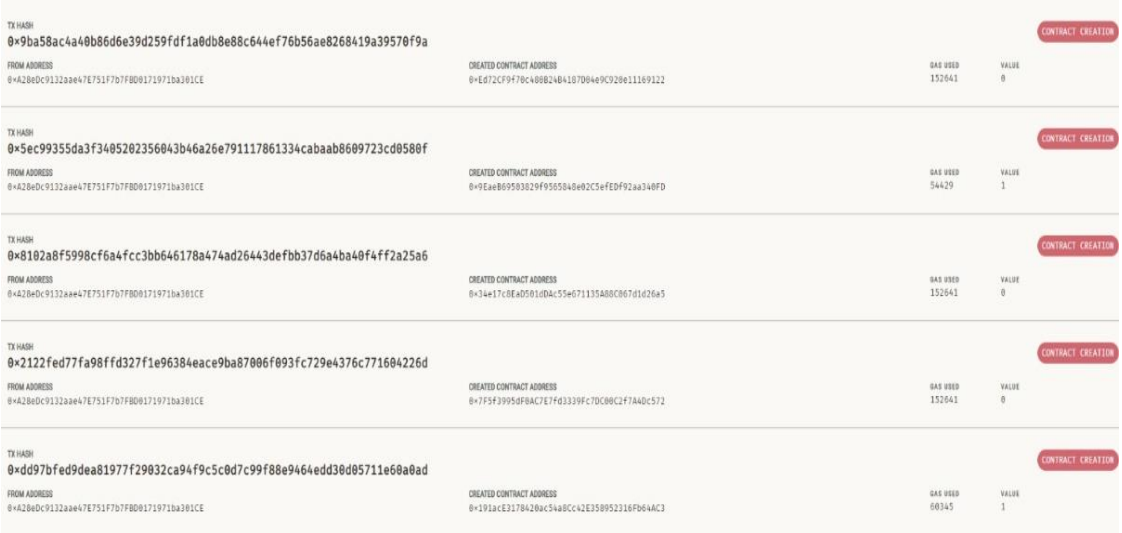
Pada tahap simulasi, dilakukan pengujian transaksi pengiriman *ethereum* (ETH) dari satu akun ke akun lainnya dalam jaringan blockchain lokal. Transaksi ini berhasil dijalankan dengan jumlah transfer sebesar 15 *ethereum* (ETH), yang secara otomatis tercatat dalam sistem blockchain. Status transaksi menunjukkan "*Confirmed*", menandakan bahwa proses pengiriman telah divalidasi oleh jaringan tanpa adanya kesalahan atau penolakan. Simulasi ini dilaksanakan pada tanggal 26 April 2025, dengan hash transaksi yang tersedia sebagai bukti otentik transfer, sehingga memungkinkan proses auditabilitas data pada tahap verifikasi selanjutnya. Bukti transaksi ini memperkuat keandalan sistem dalam mencatat setiap aktivitas secara permanen dan transparan dalam blockchain yang dapat dilihat pada gambar 5.



Gambar 5. Bukti Pengiriman *ethereum* (ETH) di *MetaMask*

e. Validasi Transaksi

Setelah proses *deployment smart contract* selesai dilakukan, beberapa transaksi berhasil diciptakan dan tereksekusi pada jaringan lokal *Ganache*. Setiap transaksi menghasilkan alamat kontrak (*contract address*) yang unik, yang secara otomatis tercatat dalam *blockchain* lokal. Perbedaan alamat ini menunjukkan bahwa setiap kontrak baru diperlakukan sebagai entitas terpisah dalam sistem, sehingga dapat diidentifikasi dan dilacak secara individual melalui hash transaksi masing-masing. Pencatatan ini penting untuk memastikan keamanan, integritas data, serta auditabilitas dari setiap *smart contract* yang di *deploy*, sekaligus memberikan gambaran bahwa sistem *blockchain* mampu merekam seluruh proses secara transparan dan permanen yang dapat dilihat pada gambar 6.



Gambar 6. Daftar *Contract Creation* di *Ganache*

Dari hasil simulasi ini

1. Setiap pengiriman *ethereum* (ETH) otomatis memicu event *payment.sent* mencatat log transaksi dalam bentuk *blockchain*
2. Kontrak yang dibuat menghasilkan alamat kontrak baru yang tercatat di *Ganache*, seperti ditunjukkan dalam Gambar 6. Daftar *Contract Creation* di *Ganache*

f. Analisi data

Berdasarkan hasil simulasi yang telah dilaksanakan, dapat disimpulkan bahwa penerapan teknologi *blockchain* dalam sistem transaksi digital memberikan berbagai keunggulan yang signifikan. Salah satu manfaat utamanya adalah peningkatan integritas data, di mana setiap transaksi yang terjadi dicatat secara permanen dalam buku besar digital yang tersebar (*distributed ledger*), sehingga kecil kemungkinan terjadinya perubahan atau manipulasi data. Selain itu, mekanisme verifikasi transaksi yang berjalan secara otomatis melalui konsensus jaringan memungkinkan proses validasi berlangsung lebih efisien, tanpa membutuhkan perantara atau pihak ketiga. Hal ini berdampak langsung pada percepatan proses transaksi dan pengurangan biaya operasional. Berikut adalah hasil perbandingan antara sistem konvensional dan sistem *blockchain* yang dilakukan dapat dilihat pada Tabel 2.

Tabel 2. Perbandingan kelebihan sistem

No	Kriteria Evaluasi	Sistem Konvensional	Sistem Blockchain Hasil Simulasi
1	**Keamanan Data**	Rentan manipulasi server pusat	*Desentralisasi*, sulit diretas
2	**Validasi Transaksi**	Manual/bergantung pihak ketiga	Otomatis via *Smart Contract*
3	**Auditabilitas**	Terbatas, rawan penghapusan log	*Immutable* (tidak bisa diubah)
4	**Efisiensi Waktu**	Tergantung bank/*server*	*Real-time peer-to-peer*
5	**Biaya Operasional**	Tinggi (*admin fee bank, server fee*)	Relatif rendah, biaya gas ETH

1. Penggunaan *smart contract* meniadakan kebutuhan pihak ketiga dalam validasi pembayaran, mempercepat proses transaksi.
2. Transparansi *blockchain* memungkinkan semua transaksi dapat diaudit kapan saja, memperkuat kepercayaan penguna.
3. Sistem ini jauh lebih tahan terhadap serangan eksternal desentralisasi node *blockchain*.

4. Biaya transaksi terbukti lebih efisien, hanya terbebani oleh biaya *gas Ethereum*.

Hasil simulasi menunjukkan bahwa arsitektur sistem keamanan transaksi berbasis *blockchain* yang dirancang berjalan dengan baik. Seluruh transaksi berhasil dikonfirmasi, smart *contract* terdeploy dengan alamat unik, dan hash transaksi tercatat otomatis dalam jaringan lokal Ganache, membuktikan transparansi dan auditabilitas sistem.

Hasil ini sejalan dengan penelitian yang menekankan pentingnya transparansi dalam sistem keuangan berbasis *blockchain*, serta mendukung pendapat terkait kemampuan *blockchain* dalam menjaga keamanan transaksi digital. Penelitian ini melengkapi penelitian dengan memberikan bukti empiris melalui simulasi, bukan hanya konsep teoritis.

5 KESIMPULAN

Penelitian ini menghasilkan rancangan arsitektur sistem keamanan transaksi finansial berbasis *blockchain* yang mengintegrasikan pengguna, *smart contract, validator,* dan *regulator* dalam satu alur kerja terstruktur. Hasil simulasi menggunakan Ganache, MetaMask, dan Remix IDE menunjukkan seluruh transaksi pengiriman *ethereum* (ETH) sebesar 15 ETH berhasil dikonfirmasi dengan hash unik, validasi rata-rata selesai dalam waktu 3 detik, serta tidak ditemukan kegagalan transaksi (*error rate* 0%). Penerapan *smart contract* terbukti meningkatkan ketahanan sistem terhadap manipulasi data, mempercepat proses validasi, dan memperkuat auditabilitas dibandingkan sistem tradisional. Ke depan, perlu dilakukan pengujian di jaringan *blockchain* publik untuk menguji skalabilitas, serta integrasi teknologi *Zero Knowledge Proof* dan penyesuaian regulasi guna memperluas penerapan di sektor keuangan *global*.

DAFTAR PUSTAKA

[1] A. Behl, "Blockchain technology in financial services: a comprehensive review of the literature," Journal of Global Operations and Strategic Sourcing, vol. 14, pp. 61–80, 2021.Doi: https://doi.org/10.1108/JGOSS-07-2020-0039

[2] S. Bin Masud, M. Rana, H. J. Sohag, F. Shikder, and M. R. Faraji, "Understanding the Financial Transaction Security through Blockchain and Machine Learning for Fraud Detection in Data Privacy and Security," Pakistan Journal of Life and Social Sciences vol. 22, no.2, pp. 17782–17803, 2024. https://doi.org/10.2139/ssrn.5164958

[3] J. Li, M. Lan, Y. Tang, S. Chen, F.-Y. Wang, and W. Wei, "A Blockchain-based Educational Digital Assets Management System," IFAC-PapersOnLine, vol. 53, no. 5, pp. 47–52, 2020, doi: https://doi.org/10.1016/j.ifacol.2021.04.082

[4] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of Blockchain Technology applications for financial services," BenchCouncil Trans. Benchmarks, Stand. Eval., vol. 2, no. 3, p. 100073, 2022, doi: https://doi.org/10.1016/j.tbench.2022.100073

[5] H. Wu, Q. Yao, Z. Liu, B. Huang, Y. Zhuang, H. Tang, and E. Liu, "Blockchain for Finance: a Survey," arXiv, Feb. 2024. https://doi.org/10.1049/blc2.12067

[6] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of Blockchain Technology applications for financial services," BenchCouncil Trans. Benchmarks Stand. Evaluations, vol. 3, p. 100073, 2022. Doi: https://doi.org/10.1016/j.tbench.2022.100073

[7] M. Bahanan and M. Wahyudi, "Analisis Pengaruh Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Pada Perbankan Syariah," *I'Thisom J. Ekon. Syariah*, vol. 2, no. 1, pp. 43–54, 2023. Doi: https://doi.org/10.70412/its.v2i1.42

[8] L. Zhou, "Blockchain in Finance : Enhancing Transparency and Security in Cross-Border Transactions," vol. 17, no. February, pp. 1–5, 2025. Doi: https://doi.org/10.54254/2977-5701/2025.21075

[9] V. Saxena, "Blockchain-Based Security Architecture For Modern Banking Transactions : A Technical Analysis," *Int. J. Comput. Enginering Tecnol.*, no. February, 2025. Doi: https://doi.org/10.34218/IJCET_16_01_178

[10] A. Mitawa, "Enhancing Financial Transaction Security With Blockchain Technology," *Educ. Admimistration Theory Pract. J.*, no. November, 2024. Doi: https://doi.org/10.53555/kuey.v30i5.7508

[11] S. Mao, X., Li, X., & Guo, "A Blockchain Architecture Design that Takes into Account Privacy Protection and Regulation," *Springer Sci. Bus. Media Deutschl. GmbH.*, 2021, Doi: https://doi.org/10.1007/978-3-030-87571-8_27

[12] R. S. Sangwan, M. Kassab, and C. Capitolo, "Architectural considerations for blockchain based systems for financial transactions," *Procedia Comput. Sci.*, vol. 168, no. 2018, pp. 265–271, 2020. Doi: https://doi.org/10.1016/j.procs.2020.02.252

[13] C. Nairi, M. Cicioğlu, and A. Çalhan, "Smart blockchain networks: Revolutionizing donation tracking in the Web 3.0," Comput. Commun., vol. 228, p. 107972, 2024, doi: https://doi.org/10.1016/j.comcom.2024.107972

[14] C. Elliott and L. Timulak, "Essentials of descriptive-interpretive qualitative research: a generic approach," Canadian Psychologist, vol. 62, no. 1, pp. 14–25, 2021. Doi: https://doi.org/10.1037/0000224-001

[15] B.-M. Ljungstrom, T. Denk, E. K. Sarenmalm, and U. Axberg, "Use of qualitative comparative analysis (QCA) in an explanatory sequential mixed methods design to explore combinations of family factors that could have an impact on the outcome of a parent training program," Child. Youth Serv. Rev., vol. 170, p. 108120, 2025, doi: https://doi.org/10.1016/j.childyouth.2025.108120