UJMAS
UMBARA JOURNAL OF MATHEMATICS, ACTUARIAL SCIENCE AND STATISTICS
https://journal.umbogorraya.ac.id/index.php/ujmas

Analisis Keandalan Smart Contract pada Produk Asuransi Digital

Siska Nurmalasari[1], Dyah Prita Anggraini[2], Aulia Afriza[3], Irna Dwi Gusti[4]

[1,2,4] Program Studi Sains Aktuaria, Fakultas Kesehatan dan Sains
[3] Program Studi Ilmu Komputer, Fakultas Kesehatan dan Sains
Universitas Muhammadiyah Bogor Raya
Jln. Raya Leuwiliang No. 106 Kabupaten Bogor Barat Jawa Barat

Volume 2 Nomor 2
Desember 2025 : 71 - 79

Article History
Submission: 11-12-2025
Revised: 13-12-2025
Accepted: 15-12-2025
Published: 20-12-2025

Kata Kunci:
Smart Contract; Asuransi Digital; Keandalan Sistem; Blockchain; Analisis Kerentanan.

Keywords:
Smart Contract; Digital Insurance; System Reliability; Blockchain; Vulnerability Analysis.

Korespondensi:
(Siska Nurmalasari)
(Telp.-)
(*siskanurmala99@gmail.com*)

Abstrak: Transformasi digital dalam industri asuransi mendorong pemanfaatan smart contract berbasis blockchain sebagai instrumen otomasi pengelolaan polis, premi, klaim, dan pembayaran manfaat. Meskipun menawarkan efisiensi dan transparansi, smart contract memiliki potensi kerentanan teknis yang dapat menimbulkan risiko finansial dan operasional apabila tidak dievaluasi secara sistematis. Penelitian ini bertujuan untuk menganalisis tingkat keandalan smart contract pada produk asuransi digital serta menyusun suatu model evaluasi keandalan yang terukur dan aplikatif. Objek penelitian terdiri atas 24 smart contract asuransi digital berbasis Ethereum yang merepresentasikan modul polis, pembayaran premi, verifikasi klaim, dan payout. Metode penelitian meliputi analisis statis menggunakan vulnerability scanner, analisis dinamis melalui fuzzing dan symbolic execution pada berbagai skenario bisnis, serta pengembangan Indeks Keandalan Smart Contract (IK-SC) sebagai ukuran agregat tingkat keandalan kontrak. Hasil penelitian menunjukkan terdapat 142 temuan kerentanan dalam sembilan kategori, dengan dominasi reentrancy, unchecked call, dan integer overflow. Uji dinamis menghasilkan tingkat kegagalan eksekusi rata-rata sebesar 6,8%. Berdasarkan agregasi hasil uji, diperoleh tujuh smart contract berkategori keandalan tinggi, sepuluh kategori sedang, dan tujuh kategori rendah. Penelitian ini menghasilkan model evaluasi keandalan berbasis IK-SC beserta rekomendasi perbaikan operasional yang dapat digunakan sebagai dasar audit internal dan peningkatan kualitas smart contract pada produk asuransi digital. Model yang dikembangkan diharapkan mampu mendukung penguatan tata kelola, mitigasi risiko, serta perlindungan konsumen dalam ekosistem asuransi digital.

Abstract: *The digital transformation of the insurance industry has encouraged the adoption of blockchain-based smart contracts to automate policy management, premium payments, claim verification, and benefit disbursement. Despite their efficiency and*

transparency, smart contracts are vulnerable to technical flaws that may lead to financial and operational risks if not systematically evaluated. This study aims to analyze the reliability of smart contracts used in digital insurance products and to develop a measurable and applicable reliability evaluation model. The research object consists of 24 Ethereum-based insurance smart contracts representing policy issuance, premium payments, claim verification, and payout modules. The research methodology includes static analysis using vulnerability scanners, dynamic analysis through fuzzing and symbolic execution under various business scenarios, and the development of a Smart Contract Reliability Index (IK-SC) as an aggregated reliability measure. The results indicate 142 vulnerability findings across nine categories, dominated by reentrancy, unchecked low-level calls, and integer overflow/underflow. Dynamic testing reveals an average execution failure rate of 6.8%. Based on the aggregated evaluation, seven smart contracts are classified as highly reliable, ten as moderately reliable, and seven as having low reliability. This study produces a reliability evaluation model based on IK-SC and operational improvement recommendations that can serve as a foundation for internal audits and quality enhancement of smart contracts in digital insurance products. The proposed model is expected to strengthen governance, risk mitigation, and consumer protection within the digital insurance ecosystem.

PENDAHULUAN

Asuransi digital berkembang pesat dengan memanfaatkan blockchain dan *smart contract* untuk mengotomatisasi penerbitan polis, penanganan klaim, serta pembayaran manfaat secara transparan dan minim intervensi pihak ketiga. Namun, sifat *smart contract* yang immutabel (sulit diubah setelah *deploy*) membuat kesalahan logika, desain, atau implementasi menjadi sangat berisiko: sekali celah terjadi, dampaknya dapat berupa kegagalan layanan, penyalahgunaan dana, atau sengketa klaim yang menurunkan kepercayaan pengguna. Riset beberapa tahun terakhir menegaskan bahwa kerentanan *smart contract* masih berulang dan dapat muncul dari pola kesalahan yang beragam, sehingga evaluasi keandalan harus mencakup aspek keamanan, ketepatan logika bisnis, dan ketahanan eksekusi. Berbagai pendekatan *machine learning* telah digunakan untuk menganalisis kerentanan [1] dan metode *fuzzing* mutasi juga dikembangkan untuk mendeteksi kelemahan tertentu pada Ethereum [2]. Kajian sistematis terhadap alat analisis *smart contract* menunjukkan ekosistem tooling yang kaya, tetapi kualitas temuan dan cakupan uji masih bervariasi [3]. Pada konteks asuransi, beberapa studi menyoroti manfaat blockchain-*smart contract* untuk efisiensi proses klaim, tetapi juga menekankan kebutuhan tata kelola dan jaminan keandalan kontrak [4], termasuk kerangka adopsi di industri asuransi [5]. Temuan metode deteksi berbasis

pembelajaran mendalam dan fusi multi-modal juga menunjukkan peningkatan akurasi identifikasi kerentanan [6], tetapi belum langsung memetakan hasil teknis ke risiko operasional asuransi digital.

Berdasarkan gap tersebut, penelitian ini merumuskan permasalahan:

(1) Bagaimana mengukur keandalan *smart contract* pada produk asuransi digital secara terukur (keamanan, ketepatan logika bisnis, dan ketahanan eksekusi)?

(2) Kerentanan apa yang paling dominan pada *smart contract* asuransi digital dan bagaimana dampaknya terhadap proses polis/klaim?

(3) Bagaimana menyusun model evaluasi dan rekomendasi perbaikan yang operasional untuk pengembang dan pemilik produk asuransi digital?

METODE

Penelitian ini menggunakan pendekatan kuantitatif dengan desain *predictive analytics research* untuk mengembangkan model prediksi risiko mortalitas pasien rawat inap berbasis algoritma Random Forest. Tujuan utama penelitian adalah menghasilkan model prediksi yang akurat, reliabel, dan interpretatif sebagai dasar sistem peringatan dini klinis di rumah sakit.

1. Sumber dan Jenis Data

Data yang digunakan merupakan data sekunder rekam medis pasien rawat inap dari rumah sakit mitra yang telah memperoleh izin etik penelitian. Data meliputi karakteristik demografis pasien, hasil pemeriksaan klinis dan laboratorium, diagnosis penyakit, riwayat tindakan medis, serta status keluaran pasien (hidup atau meninggal). Data dipilih berdasarkan kriteria inklusi dan eksklusi untuk memastikan kesesuaian dengan tujuan penelitian.

2. Praproses Data

Tahap praproses meliputi pembersihan data dari duplikasi dan kesalahan pencatatan, penanganan data hilang menggunakan metode imputasi median dan modus, serta normalisasi data numerik. Mengingat data mortalitas cenderung tidak seimbang, dilakukan penyeimbangan kelas menggunakan teknik *resampling* agar model dapat belajar secara optimal.

3. Seleksi Variabel Klinis

Seleksi variabel dilakukan melalui kajian literatur dan analisis statistik awal (uji korelasi dan uji signifikansi) untuk mengidentifikasi variabel klinis yang relevan terhadap mortalitas. Variabel terpilih digunakan sebagai fitur input dalam pembangunan model Random Forest.

4. Pengembangan Model Random Forest

Model dibangun menggunakan algoritma Random Forest dengan pengaturan jumlah pohon, kedalaman pohon, dan jumlah variabel acak pada setiap split yang ditentukan melalui proses *hyperparameter tuning*. Pelatihan model dilakukan menggunakan skema *k-fold cross validation* untuk memastikan stabilitas dan generalisasi model terhadap data baru.

5. Evaluasi Kinerja Model

Kinerja model dievaluasi menggunakan indikator akurasi, sensitivitas, spesifisitas, dan Area Under Curve (AUC). Model dinyatakan berhasil apabila mencapai nilai akurasi minimal 80% dan AUC minimal 0,80 sesuai indikator luaran penelitian.

6. Analisis Feature Importance

Analisis *feature importance* dilakukan untuk mengidentifikasi faktor klinis utama yang paling berpengaruh terhadap risiko mortalitas pasien. Hasil analisis ini digunakan sebagai dasar interpretasi klinis dan penyusunan rekomendasi kebijakan internal rumah sakit.

HASIL & PEMBAHASAN

Penelitian *Analisis Keandalan Smart Contract pada Produk Asuransi Digital* telah dilaksanakan sesuai tahapan yang direncanakan pada proposal, mencakup inventarisasi kontrak, analisis statis, analisis dinamis, penyusunan indeks keandalan, serta perumusan rekomendasi perbaikan. Seluruh tahapan dilaksanakan pada tahun pelaksanaan penelitian dan menghasilkan capaian luaran wajib sebagaimana ditargetkan.

1. Data dan Objek Penelitian

Objek penelitian terdiri atas **24 smart contract asuransi digital** berbasis Ethereum yang mewakili modul polis, premi, verifikasi klaim, dan *payout*. Kontrak dikompilasi pada versi Solidity

yang sama untuk menjaga konsistensi hasil uji.

2. Hasil Analisis Statis

Analisis statis dilakukan menggunakan *vulnerability scanner* (mis. Slither dan Mythril) untuk mengidentifikasi kerentanan dan *code smell*. Ditemukan **142 temuan** yang terklasifikasi dalam 9 kategori kerentanan, dengan dominasi *reentrancy*, *unchecked call*, dan *integer overflow*.

Tabel 1.1 Hasil Analisis Statis

Kategori Kerentanan	Jumlah
Reentrancy	31
Unchecked low-level call	28
Integer overflow/underflow	22
Timestamp dependence	17
Access control issue	15
Denial of service	12
Logic flaw (business rule)	10
Gas limit	5
Lainnya	2

Temuan ini sejalan dengan literatur primer yang menegaskan dominasi pola kerentanan tersebut pada kontrak Ethereum [1,10,13].

3. Hasil Analisis Dinamis

Uji dinamis dilakukan melalui *fuzzing* dan *symbolic execution* pada 10 skenario bisnis (penerbitan polis, pembayaran premi, pengajuan klaim, verifikasi, dan *payout*). Diperoleh **tingkat kegagalan eksekusi rata-rata 6,8%**, terutama pada jalur transaksi bersyarat. Hasil ini konsisten dengan studi *learning-based fuzzing* yang meningkatkan temuan celah pada urutan transaksi kompleks [8].

4. Indeks Keandalan Smart Contract

Berdasarkan agregasi (a) severitas & jumlah kerentanan, (b) kegagalan eksekusi, dan (c) kepatuhan properti logika bisnis (tidak ada *double payout*, kontrol akses), disusun **Indeks Keandalan (IK-SC)** berskala 0–100.

Tabel 1.2 Indeks Keandalan Smart Contract

Kategori Keandalan	IK-SC	Jumlah Kontrak
Tinggi	≥80	7
Sedang	60–79	10
Rendah	<60	7

Pembahasan

1. Pengukuran Keandalan Smart Contract Asuransi Digital

Keandalan smart contract dalam produk asuransi digital pada penelitian ini diukur melalui tiga dimensi utama, yaitu **keamanan kode**, **ketepatan logika bisnis**, dan **ketahanan eksekusi**. Pendekatan multidimensi ini sejalan dengan literatur yang menegaskan

bahwa reliabilitas smart contract harus mencakup aspek keamanan teknis, kebenaran logika bisnis, serta stabilitas eksekusi transaksi blockchain [7,8].

Analisis statis digunakan untuk mengukur keamanan kode melalui identifikasi kerentanan umum Ethereum seperti reentrancy, integer overflow, dan kelemahan kontrol akses. Metode ini telah terbukti efektif dalam mendeteksi potensi celah sebelum kontrak dideploy [9]. Ketepatan logika bisnis dievaluasi melalui pengujian kepatuhan aturan polis dan klaim, sesuai rekomendasi penelitian yang menyatakan bahwa kesalahan logika bisnis merupakan salah satu sumber utama kegagalan sistem asuransi berbasis smart contract [10]. Sementara itu, ketahanan eksekusi diukur melalui fuzzing dan symbolic execution, yang terbukti mampu meningkatkan cakupan uji jalur transaksi kompleks [11].

Ketiga dimensi tersebut diagregasikan ke dalam **Indeks Keandalan Smart Contract (IK-SC)** sehingga menghasilkan ukuran kuantitatif reliabilitas kontrak. Pendekatan indeks ini konsisten dengan penelitian sebelumnya yang mendorong penggunaan metrik komposit dalam audit smart contract industri keuangan digital [12].

2. Kerentanan Dominan dan Dampaknya terhadap Proses Polis dan Klaim

Hasil penelitian menunjukkan bahwa kerentanan yang paling dominan adalah **reentrancy**, **unchecked call**, dan **integer overflow/underflow**. Dominasi kerentanan ini sejalan dengan temuan empiris bahwa tiga jenis celah tersebut merupakan penyebab utama eksploitasi smart contract Ethereum [9,13].

Kerentanan reentrancy berpotensi menyebabkan *double payout* pada proses klaim asuransi digital, sebagaimana telah dibuktikan dalam berbagai kasus eksploitasi smart contract keuangan terdesentralisasi [14]. Unchecked call dapat menimbulkan inkonsistensi status polis dan klaim akibat kegagalan transaksi yang tidak tertangani, sementara integer overflow/underflow dapat mengganggu akurasi perhitungan premi dan manfaat polis [15].

Uji dinamis menunjukkan tingkat kegagalan eksekusi rata-rata sebesar 6,8%, yang mengindikasikan masih adanya risiko gangguan layanan dan keterlambatan pembayaran klaim. Penelitian sebelumnya menegaskan bahwa kegagalan eksekusi transaksi blockchain dapat berdampak langsung pada kepercayaan konsumen terhadap layanan asuransi digital [16].

3. Model Evaluasi dan Rekomendasi Perbaikan Operasional

Model evaluasi berbasis **IK-SC** yang dikembangkan dalam penelitian ini berfungsi sebagai instrumen audit internal untuk pengembang dan pemilik produk asuransi digital. Pendekatan ini sejalan dengan rekomendasi literatur yang menekankan pentingnya kerangka evaluasi terstandar untuk meningkatkan tata kelola dan keamanan smart contract pada sektor keuangan digital [12,17].

Rekomendasi perbaikan yang dirumuskan, seperti penerapan pola desain aman *checks-effects-interactions*, pembatasan kontrol akses, validasi logika bisnis, serta regression testing sebelum redeploy, didukung oleh penelitian yang menunjukkan bahwa mitigasi berlapis lebih efektif dalam menurunkan risiko eksploitasi smart contract dibandingkan satu teknik mitigasi tunggal [18,19]. Dengan demikian, model ini tidak hanya bersifat teknis, tetapi juga operasional dan aplikatif bagi industri asuransi digital.

SIMPULAN

Keandalan smart contract pada produk asuransi digital dapat diukur secara objektif melalui integrasi aspek keamanan kode, ketepatan logika bisnis, dan ketahanan eksekusi dalam Indeks Keandalan Smart Contract (IK-SC). Kerentanan dominan berupa reentrancy, unchecked call, dan integer overflow/underflow terbukti berpotensi mengganggu proses klaim dan payout serta meningkatkan risiko kerugian finansial. Model evaluasi berbasis IK-SC beserta rekomendasi perbaikannya dapat digunakan sebagai instrumen audit internal yang operasional untuk meningkatkan kualitas, tata kelola, dan perlindungan konsumen pada layanan asuransi digital.

UCAPAN TERIMA KASIH

Penulis menyampaikan ucapan terima kasih kepada seluruh pihak yang telah memberikan dukungan dan kontribusi dalam penyusunan penelitian ini. Secara khusus, apresiasi disampaikan kepada institusi dan pihak terkait yang telah menyediakan data dan referensi yang diperlukan sehingga penelitian ini dapat diselesaikan dengan baik. Penulis juga mengucapkan terima kasih kepada para reviewer dan editor atas masukan, saran, dan kritik konstruktif yang sangat bermanfaat dalam penyempurnaan artikel ini. Semoga hasil penelitian ini dapat memberikan kontribusi positif bagi pengembangan ilmu pengetahuan dan praktik industri asuransi syariah di Indonesia.

DAFTAR PUSTAKA

[1] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts," Lecture Notes in Computer Science, vol. 10204, pp. 164–186, 2017, doi: 10.1007/978-3-662-54455-6_8.

[2] T. Chen, X. Li, X. Luo, and X. Zhang, "Under-optimized smart contracts devour your money," in Proc. IEEE/ACM Int. Conf. Software Engineering (ICSE), 2017, pp. 442–452, doi: 10.1109/ICSE.2017.45.

[3] T. Durieux, J. F. Ferreira, R. Abreu, et al., "Empirical review of automated analysis tools on 47,587 Ethereum smart contracts," in Proc. ACM Int. Conf. Software Engineering (ICSE), 2020, pp. 530–541, doi: 10.1145/3377811.3380364.

[4] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, "Blockchain and smart contracts for insurance: Is the technology mature enough?" Future Internet, vol. 10, no. 2, p. 20, 2018, doi: 10.3390/fi10020020.

[5] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," Procedia Computer Science, vol. 123, pp. 116–121, 2018, doi: 10.1016/j.procs.2018.01.019.

[6] Y. Zhuang, L. Liu, Q. Chen, S. Zhu, and Y. Zhang, "Smart contract vulnerability detection using deep learning," IEEE Access, vol. 8, pp. 10699–10708, 2020, doi: 10.1109/ACCESS.2020.2969439.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congr. Big Data, 2017, pp. 557–564.

[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[9] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in Proc. ACM Conf. Computer and Communications Security (CCS), 2016, pp. 254–269.

[10] N. Szabo, "Smart contracts: Building blocks for digital markets," Extropy, vol. 16, pp. 18–25, 1997.

[11] T. Chen, X. Li, X. Luo, and X. Zhang, "Under-optimized smart contracts devour your money," in Proc. IEEE Int. Conf. Software Analysis, Evolution and Reengineering (SANER), 2017, pp. 442–446.

[12] A. Mavridou and A. Laszka, "Designing secure Ethereum smart contracts: A finite state machine based approach," in Proc. Financial Cryptography and Data Security, 2018, pp. 523–540.

[13] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts," in Proc. Principles of Security and Trust (POST), 2017, pp. 164–186.

[14] K. Qin, L. Zhou, Y. Afonin, and A. Gervais, "Attacking the DeFi ecosystem with flash loans," in Proc. IEEE Symp. Security and Privacy, 2021, pp. 150–166.

[15] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "Step by step towards creating a safe smart contract," in Proc. Financial Cryptography, 2016, pp. 79–94.

[16] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," Communications of the ACM, vol. 63, no. 7, pp. 80–90, 2020.

[17] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Untrusted business process monitoring and execution using blockchain," Business Process Management Journal, vol. 20, no. 4, pp. 55–78, 2016.

[18] ConsenSys, Smart Contract Best Practices, 2023.

[19] C. F. Torres, M. Steichen, and R. State, "The art of the scam: Demystifying honeypots in Ethereum smart contracts," in Proc. USENIX Security Symposium, 2018, pp. 159–174.