



INSTITUT PERTANIAN BOGOR

**PENGEMBANGAN SISTEM PENOMORAN IJAZAH DAN
SERTIFIKAT PROFESI NASIONAL (PISN)
MENGUNAKAN *BLOCKCHAIN***

TESIS

**WAHYU IBRAHIM
M0503241066**

**SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA
PROGRAM MAGISTER ILMU KOMPUTER
BOGOR
2026**



PERNYATAAN MENGENAI TESIS, SUMBER INFORMASI, PENGGUNAAN AI, DAN PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tesis dengan judul “Pengembangan Sistem Penomoran Ijazah dan Sertifikat Profesi Nasional (PISN) menggunakan *Blockchain*” merupakan salah satu syarat untuk memperoleh gelar magister pada Program Magister Ilmu Komputer. Karya ini adalah karya saya dengan arahan dari dosen pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir tesis ini.

Dalam penyusunan karya ini, saya menggunakan bantuan kecerdasan buatan Claude untuk meringkas artikel dari jurnal-jurnal terkait penelitian saya untuk dijadikan referensi. Setelah menggunakan alat/layanan tersebut, saya meninjau dan menyunting konten sesuai kebutuhan serta bertanggung jawab penuh atas isi karya tugas akhir ini.

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Institut Pertanian Bogor.

Bogor, Oktober 2026

Wahyu Ibrahim
M0503241066

© Hak Cipta milik IPB, tahun 2026
Hak Cipta dilindungi Undang-Undang

Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah, dan pengutipan tersebut tidak merugikan kepentingan IPB.

Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apa pun tanpa izin IPB.



SOROTAN

WAHYU IBRAHIM. Pengembangan Sistem Penomoran Ijazah dan Sertifikat Profesi Nasional (PISN) menggunakan *Blockchain*. Dibimbing oleh IRMAN HERMADI dan TOTO HARYANTO.

1. Penelitian ini merancang dan mengevaluasi prototipe penomoran ijazah berbasis *blockchain*.
2. Prototipe memakai Hyperledger Fabric dan penyimpanan terdistribusi melalui *Design Science Research*.
3. *Ledger* pulih otomatis dalam 9–17 detik saat *orderer leader* gagal; komponen lain belum direplikasi.
4. Jalur *chaincode* dan API memitigasi ancaman internal; celah pada tingkat infrastruktur masih ada.
5. Dua pengelola layanan menilai rancangan sangat sesuai (rerata 4,75 dari 5); bersifat deskriptif.

HIGHLIGHTS

WAHYU IBRAHIM. *Development of a Blockchain-Based National Diploma and Professional Certificate Numbering System (PISN). Supervised by IRMAN HERMADI and TOTO HARYANTO.*

1. *This study designs and evaluates a blockchain-based diploma numbering prototype.*
2. *The prototype uses Hyperledger Fabric and distributed storage through design science research.*
3. *The ledger recovers within 9–17 s after an orderer leader fails; other parts are unreplicated.*
4. *The chaincode and API path mitigates insider threats; infrastructure-level gaps remain open.*
5. *Two service managers rated the design highly appropriate (mean 4.75 of 5); results are descriptive.*



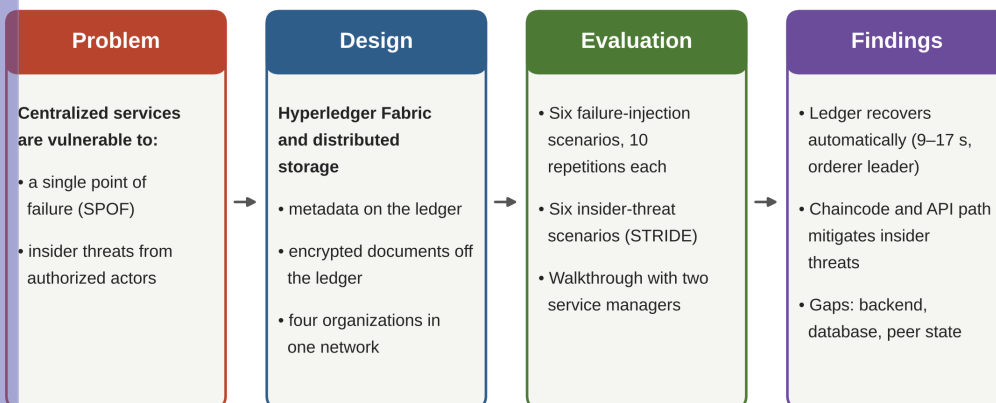
RINGKASAN VISUAL



Bukti konsep pada satu lingkungan uji; klaim ketahanan dibatasi pada lapisan *ledger*.

Penomoran Ijazah Nasional Berbasis *Permissioned Blockchain*

GRAPHICAL SUMMARY



Proof of concept in a single test environment; resilience claims limited to the ledger layer.

Permissioned Blockchain for National Diploma Numbering

RINGKASAN

WAHYU IBRAHIM. Pengembangan Sistem Penomoran Ijazah dan Sertifikat Profesi Nasional (PISN) menggunakan *Blockchain*. Dibimbing oleh IRMAN HERMADI dan TOTO HARYANTO.

Nomor ijazah nasional dan nomor sertifikat profesi nasional diterbitkan melalui sistem yang dikelola Kementerian sesuai Permendikbudristek Nomor 50 Tahun 2024; pada layanan Penomoran Ijazah dan Sertifikat Nasional (PISN) skalanya mencakup 4.303 perguruan tinggi dengan lebih dari 10 juta mahasiswa dan 2,5 juta lulusan pada tahun 2025. Arsitektur terpusat pada layanan seperti ini mengandung dua kerentanan mendasar: risiko *single point of failure* (SPOF) yang dapat melumpuhkan layanan secara keseluruhan, dan ancaman *insider threat* dari aktor berotorisasi yang tidak terdeteksi oleh kontrol keamanan berbasis perimeter.

Penelitian ini merancang, mengembangkan, dan mengevaluasi *proof of concept* (PoC) arsitektur PISN berbasis Hyperledger Fabric 2.5 dan penyimpanan terdistribusi dengan IPFS, menggunakan pendekatan *Design Science Research*, dengan metadata transaksi disimpan *on-chain* dan dokumen pendukung terenkripsi disimpan *off-chain*. Artefak didemonstrasikan pada empat proses bisnis inti penerbitan standar, penerbitan via eksepsi, pencabutan (rancangan penelitian), dan verifikasi publik yang melibatkan empat aktor institusional (Perguruan Tinggi, Kemdiktisaintek, LLDikti, Kemenag) dalam satu jaringan *permissioned blockchain*.

Ketahanan terhadap SPOF pada lapisan *ledger* diuji melalui enam skenario injeksi kegagalan (*fault injection*) pada *peer* dan *orderer*, ditambah satu skenario *baseline* sebagai kontrol, masing-masing diulang sepuluh kali. Kegagalan satu *orderer follower* tidak mengganggu penulisan, sedangkan kegagalan *orderer leader* menghentikan penulisan sementara selama sekitar 9 sampai 17 detik sebelum pulih otomatis. Kehilangan kuorum menghentikan *commit* dan pulih otomatis dalam sekitar 15 detik setelah kuorum kembali. Ketahanan pada lapisan *peer* bersifat asimetris mengikuti *endorsement policy* AND(PT, OR(regulator)): kegagalan satu *peer* regulator dikompensasi tanpa penalti latensi yang teramati, sedangkan kegagalan *peer* perguruan tinggi menghentikan penerbitan tanpa *failover*. Komponen di luar *ledger* (*backend*, PostgreSQL, dan IPFS) tidak direplikasi dan teramati menjadi SPOF pada lapisan aplikasi, sehingga klaim ketahanan penelitian ini dibatasi pada lapisan *ledger* dan pada kegagalan *node* individual di satu lingkungan uji.

Mitigasi *insider threat* dievaluasi melalui enam skenario (T1, T2, T3, T4, T5a, dan T5b) pada tiga kategori STRIDE yang paling terkait penyalahgunaan hak akses oleh aktor internal, yaitu *Tampering*, *Elevation of Privilege*, dan *Repudiation*, dengan berpegang pada model *adversary* dan batas kepercayaan yang didefinisikan lebih dulu. Tiga kategori lain (*Spoofing*, *Information Disclosure*, dan *Denial of Service*) ditinjau ulang dan hanya diamati atau diuji sebagian. Pada jalur transaksi yang melewati *chaincode* dan API, upaya memaksakan definisi *chaincode* oleh satu organisasi ditolak oleh *lifecycle governance* multi-organisasi (T1), penerbitan tanpa atribut peran ditolak *chaincode* (T3), tindakan lintas yurisdiksi ditolak pada dua lapis independen, yaitu *backend* dan *chaincode* (T4), dan riwayat *on-chain* tidak dapat dihapus melalui *chaincode* (T5a). Perubahan *record* melalui *chaincode* dicegah oleh *hash* yang dihitung di *chaincode*, tetapi substitusi dokumen hanya



Hak Cipta Dilindungi Undang-undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

terdeteksi apabila *hash* dibandingkan dengan sumber tepercaya (T2). Pencegahan ini tidak berlaku pada tingkat infrastruktur: *state database peer* terbuka dengan kredensial bawaan dan dapat diubah tanpa transaksi (T5b); *endorsement* multi-organisasi tetap menolak transaksi yang bertumpu pada *state* yang diubah, tetapi karena verifikasi publik membaca melalui satu *peer*, perubahan itu dapat memunculkan status verifikasi yang keliru; selain itu satu *backend* memegang identitas seluruh organisasi. Kedua celah residual tersebut belum ditutup pada PoC.

Masukan formatif atas relevansi rancangan dikumpulkan melalui evaluasi kontekstual bersama dua pengelola layanan PISN di Direktorat Pembelajaran dan Kemahasiswaan, Kemdiktisaintek, menggunakan *walkthrough* terstruktur dan kuesioner Likert lima poin pada empat dimensi yang berkorespondensi dengan kriteria desain. Seluruh butir dinilai pada kisaran 4 sampai 5, dengan rata-rata keseluruhan 4,75 (Sangat Sesuai) dan skor tertinggi pada dimensi kesesuaian alur otorisasi antar-aktor (5,00). Karena responden hanya dua orang dari satu unit kerja dan penilaian diberikan sebelum pengujian berulang, hasil ini bersifat deskriptif dan tidak digeneralisasi.

Kontribusi utama penelitian terletak pada integrasi konteks regulasi PISN yang konkret, evaluasi ketahanan lapisan *ledger* yang terukur melalui injeksi kegagalan berulang, dan evaluasi mitigasi *insider threat* berbasis desain *permissioned blockchain* terdistribusi yang menyatakan secara terbuka batas pencegahannya (jalur *chaincode* dan API) serta celah residual pada tingkat infrastruktur, melengkapi kajian terdahulu yang umumnya bertumpu pada asumsi arsitektural tanpa pengujian kegagalan node, dan pada analisis ancaman yang berorientasi deteksi atau belum disertai percobaan serangan.

SUMMARY

WAHYU IBRAHIM. *Development of a Blockchain-Based National Diploma and Professional Certificate Numbering System (PISN). Supervised by IRMAN HERMADI and TOTO HARYANTO.*

National diploma numbers and national professional certificate numbers are issued through a system managed by the Ministry, in accordance with Regulation of the Minister of Education, Culture, Research, and Technology (Permendikbudristek) No. 50 of 2024; the scale of the National Diploma and Professional Certificate Numbering (PISN) service covers 4,303 higher education institutions, more than 10 million enrolled students, and 2.5 million graduates in 2025. Centralized architectures for services of this kind carry two fundamental vulnerabilities: a single point of failure (SPOF) risk that can incapacitate the entire service, and insider threat from authorized actors that perimeter-based security controls do not detect.

This study designs, develops, and evaluates a proof-of-concept (PoC) PISN architecture based on Hyperledger Fabric 2.5 and IPFS-based distributed storage, using a Design Science Research approach, with transaction metadata stored on-chain and encrypted supporting documents stored off-chain. The artifact is demonstrated across four core business processes: standard issuance, exception-based issuance, revocation (a research design), and public verification. Four institutional actors take part within a single permissioned blockchain network:



higher education institutions, the Ministry of Higher Education, Science, and Technology (Kemdiktisaintek), the Regional Office for Higher Education (LLDikti), and the Ministry of Religious Affairs (Kemenag).

SPOF resilience at the ledger layer is tested through six failure-injection scenarios on peers and orderers, plus a baseline control scenario, each repeated ten times. The failure of a single follower orderer does not disrupt writes, whereas the failure of the leader orderer suspends writes for roughly 9 to 17 seconds before automatic recovery. Loss of quorum halts commits and recovers automatically within about 15 seconds after quorum is restored. Peer-layer resilience is asymmetric and follows the endorsement policy AND(HEI, OR(regulator)), where HEI is the higher education institution peer: the failure of a single regulator peer is compensated with no observable latency penalty, whereas the failure of the HEI peer halts issuance without failover. Components outside the ledger (backend, PostgreSQL, and IPFS) are not replicated and were observed to be single points of failure at the application layer; the resilience claim of this study is therefore limited to the ledger layer and to the failure of individual nodes in a single test environment.

Insider-threat mitigation is evaluated through six scenarios (T1, T2, T3, T4, T5a, and T5b) on the three STRIDE categories most closely tied to misuse of access rights by internal actors, namely Tampering, Elevation of Privilege, and Repudiation, based on an adversary model and trust boundaries defined beforehand. The other three categories (Spoofing, Information Disclosure, and Denial of Service) were reviewed, but only through observation or partial testing. On the transaction path that passes through the chaincode and the API, an attempt by a single organization to force a chaincode definition is rejected by multi-organization lifecycle governance (T1), issuance without a role attribute is rejected by the chaincode (T3), cross-jurisdiction actions are rejected at two independent layers, the backend and the chaincode (T4), and the on-chain history cannot be deleted through the chaincode (T5a). Changes to a record through the chaincode are prevented by a hash computed in the chaincode, but document substitution is detected only when the hash is compared against a trusted source (T2). This prevention does not extend to the infrastructure level: the peer state database is exposed with default credentials and can be modified without a transaction (T5b). Multi-organization endorsement still rejects transactions that rely on the altered state, but because public verification reads through a single peer, the change can produce an incorrect verification status. In addition, a single backend holds the identities of all organizations. These two residual gaps remain open in the PoC.

Formative input on the relevance of the design was collected through a contextual evaluation with two PISN service managers at the Directorate of Learning and Student Affairs, Ministry of Higher Education, Science, and Technology (Kemdiktisaintek), using a structured walkthrough and a five-point Likert questionnaire across four dimensions corresponding to the design criteria. All items were rated between 4 and 5, with an overall mean of 4.75 (Highly Appropriate) and the highest score (5.00) on the dimension of actor-authorization-flow appropriateness. Because there were only two respondents from a single work unit and the ratings were given before the repeated tests, the results are descriptive and cannot be generalized.

The main contribution of this study lies in the integration of a concrete PISN regulatory context, a measurable evaluation of ledger-layer resilience through



1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

repeated failure injection, and an evaluation of by-design insider-threat mitigation on a distributed permissioned blockchain. The study states openly the limits of its prevention (the chaincode and API path) and the residual gaps at the infrastructure level. Together, these complement prior studies that generally rely on architectural assumptions without node-failure testing, and on threat analyses that are detection-oriented or not accompanied by attack attempts.

Kata kunci: *design science research, Hyperledger Fabric, insider threat, PISN, single point of failure*

Keywords: *design science research, Hyperledger Fabric, insider threat, PISN, single point of failure*



@Hak cipta milik IPB University

IPB University



IPB University
— Bogor Indonesia —

Hak Cipta Dilindungi Undang-undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

Penguji pada Ujian Tesis:
Dr. Shelve Nidya Neyman, S.Kom., M.Si.



@Hak cipta milik IPB University

IPB University



IPB University
— Bogor Indonesia —

Hak Cipta Dilindungi Undang-undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

Perpustakaan IPB University



Judul Tesis : Pengembangan Sistem Penomoran Ijazah dan Sertifikat Profesi Nasional (PISN) menggunakan *Blockchain*

Nama : Wahyu Ibrahim

NIM : M0503241066

Disetujui oleh

Pembimbing 1:
Irman Hermadi, S.Kom., M.S., Ph.D.



Pembimbing 2:
Dr. Toto Haryanto, S.Kom., M.Si.



Diketahui oleh

Ketua Program Magister Ilmu Komputer:
Dr. Toto Haryanto, S.Kom., M.Si.
NIP 198211172014041001



Dekan Sekolah Sains Data, Matematika, dan Informatika:
Prof. Dr. Ir. Agus Bueno, M.Si., M.Kom.
NIP 196607021993021001



Tanggal Ujian: 24 September 2026

Tanggal Lulus:



PRAKATA

Puji dan syukur penulis panjatkan kepada Allah subhanaahu wa ta'ala atas segala karunia-Nya sehingga karya ilmiah ini berhasil diselesaikan. Tema yang dipilih dalam penelitian yang dilaksanakan sejak bulan Juli 2025 sampai bulan September 2026 ini ialah sistem pemerintahan berbasis elektronik, dengan judul "Pengembangan Sistem Penomoran Ijazah dan Sertifikat Profesi Nasional (PISN) menggunakan *Blockchain*".

Terima kasih penulis ucapkan kepada para pembimbing yaitu Bapak Irman Hermadi, S.Kom., M.S., Ph.D. selaku ketua pembimbing dan Bapak Dr. Toto Haryanto, S.Kom., M.Si. selaku anggota pembimbing yang telah membimbing dan banyak memberi saran. Ucapan terima kasih juga disampaikan kepada komisi pembimbing, moderator ujian tesis Ibu Rina Trisminingsih, S.Kom., M.T., Ph.D. dan penguji luar komisi pembimbing Ibu Dr. Shelve Nidya Neyman, S.Kom., M.Si. Di samping itu, penghargaan penulis sampaikan kepada Bapak Dr. Beny Bandanadjaja, S.T., M.T., Direktur Pembelajaran dan Kemahasiswaan yang telah memberikan izin untuk melaksanakan tugas belajar, Bapak Andhika Ganendra, S.Si., M.M., Kepala Pusat Layanan Pembiayaan Pendidikan, Kemdikbudristek yang telah memberikan Beasiswa Unggulan Kategori Pegawai, Bapak Kevin Leonard Michael Marbun, S.E., M.A., Kepala Subdirektorat Penjaminan Mutu, Direktorat Pembelajaran dan Kemahasiswaan, Ibu Dhaniek Wardhanie Ratnaningrum, S.S., Saudara Rifqi A'zhom Muta'allimin, S.Pd., dan Saudara Prima Kresnala, S.Kom., M.T.I., yang telah memberikan bantuan dan dukungan selama pengumpulan data. Ungkapan terima kasih juga disampaikan kepada Bapak Kamisan, dan Ibu Siti Rohani, adik-adikku Novi Zasinta Pahlawani, Dara Rosani, dan Akbar Sulaiman, serta istri tercinta Ike Kencana Sari, anak Abdullah Hanif Wicaksono Ibrahim dan Muhammad Ammar Pradityo Ibrahim yang telah memberikan dukungan, doa, dan kasih sayang.

Semoga karya ilmiah ini bermanfaat bagi pihak yang membutuhkan dan bagi kemajuan ilmu pengetahuan.

Bogor, Oktober 2026

Wahyu Ibrahim

DAFTAR ISI

DAFTAR TABEL	xiv
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xiv
I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan	4
1.4 Manfaat	4
1.5 Ruang Lingkup	4
II TINJAUAN PUSTAKA	6
2.1 <i>E-Government</i> dan Sistem Penomoran Kredensial	6
2.2 <i>Permissioned Blockchain</i> dan Konsensus Raft	6
2.3 Hyperledger Fabric	7
2.4 <i>InterPlanetary File System</i> (IPFS)	8
2.5 <i>Blockchain</i> untuk <i>E-Government</i>	8
2.6 Hyperledger Fabric dan IPFS untuk Dokumen dan Kredensial	8
2.7 <i>Single Point of Failure</i> (SPOF) pada Arsitektur Layanan	9
2.8 <i>Insider Threat</i> dan Auditabilitas	9
2.9 <i>Design Science Research</i> (DSR) pada Artefak <i>Blockchain</i>	10
2.10 Perbandingan Penelitian Terkait	10
2.11 <i>Research Gap</i> dan Posisi Penelitian	11
III METODE	12
3.1 Lokasi dan Sumber Data Penelitian	12
3.2 Tahapan Penelitian	13
3.3 Lingkungan Pengembangan	21
3.4 Analisis Data	21
IV HASIL DAN PEMBAHASAN	23
4.1 Demonstrasi Prototipe	23
4.2 Evaluasi Ketahanan Infrastruktur terhadap SPOF	29
4.3 Evaluasi Mitigasi Ancaman Internal Berbasis STRIDE	38
4.4 Evaluasi Kontekstual Formatif (Masukan Relevansi Artefak)	51
4.5 Keterbatasan Penelitian	57
V SIMPULAN DAN SARAN	61
5.1 Simpulan	61
5.2 Saran	61
DAFTAR PUSTAKA	63
LAMPIRAN	68
RIWAYAT HIDUP	108

DAFTAR TABEL

1	Tinjauan literatur dari penelitian terkait	10
2	Rancangan pengujian ketahanan SPOF	18
3	Rancangan pengujian mitigasi <i>insider threat</i> berbasis STRIDE	19
4	Lingkungan pengembangan	21
5	Ringkasan hasil demonstrasi prototipe per skenario (1 Juli 2026)	24
6	Hasil skenario injeksi kegagalan <i>peer</i> (N = 10 per skenario, 28 September 2026)	32
7	Hasil skenario injeksi kegagalan <i>orderer</i> (N = 10 per skenario, 28 September 2026)	34
8	Dampak kegagalan komponen di luar <i>ledger</i> (satu gangguan per komponen, tiga ronde <i>probe</i>)	35
9	Perbandingan arsitektur terpusat (konseptual) dan terdistribusi PoC	37
10	Kelas <i>adversary</i> dan kapabilitasnya	39
11	Batas kepercayaan, kontrol yang ada, dan ancaman dominan	40
12	Tinjauan ulang kategori STRIDE yang semula dikeluarkan	40
13	Riwayat transaksi nomor PISN 001002142012026100003 (<i>block height</i> tetap 393 selama pengujian)	47
14	Rangkuman hasil evaluasi skenario STRIDE	50
15	Profil responden evaluasi kontekstual formatif	53
16	Hasil penilaian kuesioner evaluasi kontekstual formatif (n = 2)	53
17	Skor butir terpilih dibandingkan dengan temuan teknis	55

DAFTAR GAMBAR

1	Infografis statistik pendidikan tinggi tahun 2025 (PDDikti Kemdiktisaintek 2026)	1
2	Proses bisnis layanan PISN, diolah dari Kemdiktisaintek (2025a)	6
3	Komponen-komponen yang menyusun Hyperledger Fabric, diolah dari Hyperledger Foundation (2023b)	7
4	Alur tahapan penelitian dengan metode DSR, diolah dari Peffers <i>et al.</i> (2007)	14
5	Arsitektur artefak PISN berbasis Hyperledger Fabric dan IPFS	15
6	Alur transaksi penerbitan nomor PISN	16
7	Alur pengembangan iteratif artefak/prototipe	17

DAFTAR LAMPIRAN

1	Tangkapan Layar antarmuka prototipe sistem PISN dan respons API demonstrasi	68
2	Instrumen Kuesioner Evaluasi Kontekstual <i>Stakeholder</i>	79
3	Data hasil dan Perhitungan Kuesioner Evaluasi Kontekstual	83
4	Catatan tanya-jawab <i>walkthrough</i> evaluasi kontekstual	85
5	Bukti Pengujian Ketahanan SPOF dan Mitigasi STRIDE	88