

Madani: Jurnal Ilmiah Multidisiplin
Volume 3, Nomor 10, November 2025, P. 201-209
E-ISSN: 2986-6340
Licensed by CC BY-SA 4.0
DOI: <https://doi.org/10.5281/zenodo.17775383>

Penerapan Teknologi *Blockchain* Pada Sistem *Financial Technology* Sebagai Upaya Preventif Pencegahan Kebocoran Data Pribadi

The Application of Blockchain Technology in Financial Technology Systems as a Preventive Effort to Prevent Personal Data Leakage

Vaganti Safa Sukma Rubianti

¹Fakultas Hukum, Universitas Pembangunan Nasional Veteran Jakarta
 Email : 2210611439@mahasiswa.upnvj.ac.id

Abstrak

Pada era digitalisasi seperti sekarang banyak sekali kemudahan yang tersedia. Kita dapat melakukan segala aktivitas di internet mulai dari belajar, bermain, berbelanja, dan membayar iuran seperti PBB, Biaya pendidikan, dan listrik. Kita tidak perlu repot menyimpan banyak uang di dompet karena pembayaran dapat dilakukan secara online dengan financial technology. Penelitian ini bertujuan untuk mencari tahu seberapa besar peluang diterapkannya teknologi blockchain sebagai upaya preventif atau pencegahan kebocoran data pribadi pada sistem financial technology. Penelitian ini menggunakan metode penelitian yuridis normatif dengan pendekatan undang undang dan konseptual untuk menguji kepastian hukum jika teknologi blockchain diterapkan dalam sistem financial technology. Hasil penelitian menunjukkan bahwa blockchain menawarkan sistem pengamanan yang aman dan tidak mudah diretas karena sifatnya desentralisasi dan immutable. Maka, tidak ada yang bisa memanipulasi atau memusnahkan data transaksi yang dicatat dalam blok. Namun, karena sifat immutable dan desentralisasi menjadi tantangan dalam pemenuhan hak subjek data pribadi. Diperlukan upaya kolaborasi pemerintah dan penyelenggara layanan financial technology untuk memperkuat regulasi dan infrastruktur teknologi blockchain, agar tercipta kepastian hukum serta sistem keamanan yang kuat dan dapat memitigasi risiko kebocoran data pribadi.

Kata Kunci : *Financial Technology, Blockchain, dan Data Pribadi*

Abstract

In today's digital era, conveniences abound. We can conduct all activities online, from studying and playing, shopping, and paying taxes such as property tax (PBB), education fees, and electricity. We no longer need to carry large amounts of cash in our wallets because payments can be made online using financial technology. This study aims to determine the potential for implementing blockchain technology as a preventative measure against personal data leaks in financial technology systems. This study uses a normative juridical research method with a legal and conceptual approach to test the legal certainty of blockchain technology's application in financial technology systems. The results show that blockchain offers a secure and hack-resistant security system due to its decentralized and immutable nature. Therefore, no one can manipulate or destroy transaction data recorded in blocks. However, this immutable and decentralized nature presents challenges in fulfilling the rights of personal data subjects. Collaborative efforts are needed between the government and financial technology service providers to strengthen blockchain technology regulations and infrastructure to create legal certainty and a robust security system that can mitigate the risk of personal data leaks.

Keywords: *Financial Technology, Blockchain, and Personal Data*

Article Info

Received date: 25 Oktober 2025

Revised date: 15 November 2025

Accepted date: 25 November 2025

PENDAHULUAN

Pada era globalisasi seperti sekarang segala kebutuhan dapat dipenuhi dengan mudah. Kita bisa belanja, membeli makanan, dan menonton hanya dengan smartphone dan bantuan internet. Berdasarkan laporan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada kuartal 2 tahun 2025

pengguna internet di Indonesia mencapai 229,5 Juta angka tersebut terus mengalami kenaikan sejak tahun 2023 sekitar 215,5 juta jiwa dan 221,5 juta jiwa pada tahun 2024. Fenomena tersebut menunjukkan bahwa semakin bertambah masyarakat yang mengandalkan internet untuk menjalani aktivitas sehari-hari, mulai dari aktivitas sosial seperti berkomunikasi satu sama lain maupun aktivitas ekonomi seperti jual beli.¹

Memasuki era digitalisasi 4.0 yang terus mengalami perubahan turut merubah cara seseorang dalam bertransaksi, dulu jual beli hanya dapat dilakukan dengan cara datang ke toko langsung dan membayar dengan uang konvensional. Namun, sekarang kita dapat membeli barang melalui aplikasi *E-Commerce* dengan metode pembayaran yang beragam seperti transfer melalui *Mobile Banking*, qris, dan *Cash On Delivery* (COD). setelah melakukan pembayaran kita hanya tinggal menunggu barang diantar ke rumah melalui jasa ekspedisi tanpa repot mengambil barang ke penjual. Dengan adanya e-commerce proses transaksi semakin mudah, dengan banyak nya metode pembayaran yang tersedia kita tidak perlu memegang uang cash yang memakan banyak tempat.²

Kemudahan pembayaran tidak hanya dalam e-commerce, kita juga dapat melakukan pembayaran non tunai saat membeli makanan dan minuman di restoran dan warung, zaman sekarang sudah banyak warung kecil yang menerima pembayaran dengan qris dari semua bank dan dompet digital seperti Ovo Gopay, dan Shopee pay. Contoh lainnya adalah kemudahan dalam membeli tiket perjalanan kereta, dulu kita harus antri panjang ke loket untuk membeli tiket. Namun sekarang kita dapat memindai kode di pintu masuk tanpa perlu antri panjang di loket. Kemudahan metode pembayaran yang kita rasakan saat ini merupakan inovasi di sektor keuangan atau yang dapat kita sebut dengan financial technology (fintech). Fintech adalah inovasi layanan di bidang jasa keuangan yang memanfaatkan teknologi untuk mempermudah, mempercepat, dan meningkatkan akses masyarakat terhadap produk keuangan. Contoh financial technology meliputi dompet digital seperti Gopay, Ovo, dan Shoppe pay. Platform pinjaman online seperti Kredivo, Akulaku, Tunaiku, dan Danabijak. Mobile banking seperti Brimo (BRI), Wondr (BNI), Byond (BSI), Livin (Mandiri), dan BCA Mobile.³

Semakin banyak inovasi di bidang keuangan atau fintech, kita tidak perlu repot membawa uang di dompet dengan jumlah banyak yang memakan tempat dan berat, uang konvensional rentan akan pencurian dan hilang karena terjatuh, selain itu uang konvensional juga mudah rusak jika terkena air dan banyak orang yang tidak mau menerima jika uang rusak. Maka dari itu banyak masyarakat yang beralih pada sistem pembayaran digital, cukup membawa handphone kita dapat melakukan pembayaran di banyak toko. Berdasarkan data dari Bank Indonesia transaksi dengan qris mengalami pertumbuhan signifikan sebanyak 154, 86 % pada kuartal 2 tahun 2025.⁴

Perlu diingat bahwa perkembangan teknologi bagaikan pisau bermata dua yang dapat memberikan kenikmatan dan ancaman secara bersamaan. Ancaman yang kita hadapi dengan perkembangan fintech adalah kebocoran data pribadi seperti no. rekening, pin, dan sandi yang kerap kali menyebabkan kehilangan saldo dan merugikan seperti yang terjadi pada 15 Juta nasabah Bank Syariah Indonesia yang kehilangan data dan menderita kerugian karena sistem diretas oleh hacker lockbit dan dijual melalui dark web. Kebocoran data terjadi karena sistem yang kurang kuat sehingga rentan terkena serangan seperti malware, ransomware, dan spyware.⁵

¹ Palinggi, S., & Limbongan, E. C. (2020, January). Pengaruh internet terhadap industri ecommerce dan regulasi perlindungan data pribadi pelanggan di Indonesia. In *Semnas Ristek (Seminar Nasional Riset Dan Inovasi Teknologi)* (Vol. 4, No. 1).

² Kurniati, R. R., & Junaida, D. (2019). Pengaruh E-Commerce Terhadap Keputusan Pembelian Pada Belanja Online Shopee (Studi Pada Konsumen Belanja Online Mahasiswa Universitas Islam Malang). *JIAGABI (Jurnal Ilmu Administrasi Niaga/Bisnis)*, 8(3), 154-162.

³ Purwanto, H., Yandri, D., & Yoga, M. P. (2022). Perkembangan dan dampak financial technology (fintech) terhadap perilaku manajemen keuangan di masyarakat. *Kompleksitas: Jurnal Ilmiah Manajemen, Organisasi Dan Bisnis*, 11(1), 80-91.

⁴ Utomo, S., Safuan, S., & Alhabsy, M. A. (2023). Implementasi kebijakan penggunaan QRIS terhadap praktik UMKM sebagai upaya percepatan pertumbuhan ekonomi digital.

⁵ Bakri, A. A., Hasanah, N., & Lasmiatun, K. M. T. (2024). Financial technology innovation and banking industry transformation: A literature study on financial markets. *Multifinance*, 1(3), 230-238.

Melihat kerentanan pencurian data pribadi maka penerapan teknologi blockchain pada sistem financial technology dapat menjadi solusi untuk mencegah terjadinya serangan yang menyebabkan kebocoran data pribadi. Blockchain merupakan sistem komputer yang memiliki karakteristik transparan, desentralisasi, dan immutable. Blockchain bagaikan buku besar digital yang dapat dilihat oleh semua yang ada di jaringan dan setiap pencatatan dilakukan secara real time sehingga lebih transparan dan aman karena semua orang dapat mengetahui jika terjadi transaksi baru sehingga dapat mencegah kecurangan atau pencurian selain itu blockchain juga desentralisasi jadi dapat terhindar dari serangan hacker karena sistem dikendalikan banyak orang bukan hanya oleh satu otoritas. Berdasarkan permasalahan yang telah dijelaskan, maka penulis menarik dua rumusan masalah. Yakni, apa keunggulan dan keterbatasan blockchain dalam mencegah kebocoran data pribadi pengguna fintech dan bagaimana kepatuhan sistem fintech berbasis blockchain terhadap UU PDP & UU ITE di Indonesia.⁶

METODE PENELITIAN

Metode penelitian adalah cara untuk mengumpulkan dan mengolah data guna menjawab masalah dalam penelitian.⁷ Pada penelitian kali ini penulis menggunakan metode yuridis normatif yang berfokus pada pengujian bagaimana keefektifan penerapan bahan hukum primer seperti peraturan perundang undangan di masyarakat dengan cara menemukan kaidah hukum yang dapat menyelesaikan permasalahan hukum yang terjadi melalui penelitian terdahulu. Penelitian ini menggunakan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach)

HASIL DAN PEMBAHASAN

Keunggulan dan Keterbatasan Blockchain Dalam Mencegah Kebocoran Data Pribadi Pengguna *Financial Technology*

Data pribadi adalah segala informasi yang berkaitan dengan seorang individu atau suatu informasi yang dapat mengidentifikasi seseorang secara langsung maupun tidak langsung. Di Indonesia data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP).⁸ pada pasal 4 UU PDP menjelaskan bahwa data pribadi terbagi menjadi data pribadi umum dan data pribadi spesifik. Nama, tempat tanggal lahir, kewarganegaraan, Agama, Jenis kelamin, dan Status perkawinan termasuk data pribadi umum. Sedangkan data pribadi khusus mencakup data dan informasi kesehatan, data biometrik, data anak, dan data riwayat kejahatan.⁹ Proses penyimpanan data pribadi melibatkan 3 pihak. Yakni, pemilik data, pengendali data, dan prosesor data pribadi. Pengendali data merupakan pihak yang menentukan tujuan dan memegang kendali atas pemrosesan data pribadi, perusahaan financial technology (Fintech) merupakan contoh dari pengendali data karena fintech mengendalikan data pribadi seperti nama, NIK, foto, data transaksi, dan data biometrik seluruh pengguna. Penyimpanan data bertujuan untuk merealisasikan sistem keuangan anti pencucian uang dan pencegahan pendanaan terorisme yang diamanatkan pada pasal 6 Peraturan Bank Indonesia Nomor 19 tahun 2010.¹⁰

Sebagai bentuk realisasi praktik sistem keuangan anti pencucian uang dan pencegahan pendanaan terorisme penyelenggara jasa keuangan diwajibkan untuk melakukan customer due diligence atau *know your customer* dengan mengidentifikasi nasabah dengan cara mengumpulkan data nasabah

⁶ Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia: Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, 3(2), 145-160.

⁷ Zainuddin, M., & Karina, A. D. (2023). Penggunaan metode yuridis normatif dalam membuktikan kebenaran pada penelitian hukum. *Smart Law Journal*, 2(2), 114-123.

⁸ Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan data pribadi warga negara Indonesia terkait dengan kebocoran data. *Jurnal Kewarganegaraan*, 6(1), 976-982.

⁹ Pasal 4 Undang-Undang Nomor 27 Tahun 2022

¹⁰ Pakpahan, J. M. (2024). Kesadaran Urgensi Peran Pengendali Dan Prosesor Data Pribadi Dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Hukum to-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat*, 10(1), 119-137.

seperti nama, alamat, KTP, pas foto, no. telepon, pekerjaan, penghasilan, tujuan membuka rekening, sumber dana dan alamat. Setelah dikumpulkan bank akan memverifikasi apakah data yang dimasukkan oleh customer valid atau tidak dan mencocokkan tanda tangan.¹¹ Seluruh data nasabah akan disimpan dalam penyimpanan yang bersifat sentralisasi dan dikendalikan oleh otoritas. Sistem keamanan bank menggunakan sistem *Two Factor Authentication* atau sistem keamanan yang membutuhkan dua langkah verifikasi contohnya dengan *Password* dan OTP atau PIN dan Biometrik (sidik jari dan wajah). Namun, meskipun perbankan sudah menggunakan sistem keamanan dua langkah akan tetapi masih disimpan dalam server yang terpusat makanya server masih rentan terkena malware atau ransomware dan data nasabah mudah dicuri oleh oknum yang tidak bertanggung jawab. Data yang dicuri akan dijual di situs dark web.¹²

Blockchain merupakan teknologi buku besar yang terdesentralisasi dan menyimpan data secara aman dan transparan dalam jaringan komputer. Setiap transaksi akan tersimpan dalam sebuah blok yang dikunci dengan kunci privat atau hash. Setiap transaksi yang dicatat dalam blockchain disambungkan dengan rantai (*chain*) yang berisi kunci privat atau hash dari blok sebelumnya. Blockchain ada 2 jenis yakni blockchain publik dan privat. Blockchain publik adalah blockchain yang dapat diakses oleh siapa saja tanpa perlu izin tertentu, blockchain jenis ini sering digunakan dalam kriptografi. Sedangkan blockchain privat adalah blockchain yang hanya dapat diakses oleh pihak yang sudah mendapatkan izin dari pihak yang berwenang. Berbeda dengan blockchain publik yang dapat diakses oleh siapa saja, blockchain privat dikendalikan oleh satu pihak.¹³ Blockchain bersifat desentralisasi atau tidak terpusat, setiap transaksi di dalam blockchain akan diketahui oleh seluruh pengguna yang ada di jaringan, sifat inilah yang membuat blockchain menjadi transparan, sifat ini dapat memitigasi risiko kebocoran data pribadi karena semua transaksi akan diketahui dan divalidasi bersama sama oleh pengguna yang ada di jaringan.

Dalam proses penyimpanan data pribadi pada layanan fintech, blockchain menawarkan struktur keamanan yang jauh berbeda dengan model sentralisasi tradisional. Pertama, sifat desentralisasi blockchain memberikan perlindungan yang lebih kuat terhadap risiko *single point of failure*, yaitu kondisi di mana satu server yang diretas dapat menyebabkan kebocoran data dalam jumlah besar. Model sentralisasi ini menjadi salah satu kelemahan terbesar sistem elektronik, sebagaimana diatur dalam Pasal 14 ayat (1) PP 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang mewajibkan Penyelenggara Sistem Elektronik (PSE) menyediakan keamanan yang memadai untuk melindungi data pribadi. Blockchain secara inheren memenuhi prinsip keamanan tersebut karena data tersebar dalam banyak node, sehingga serangan pada satu titik tidak langsung mengkompromikan seluruh sistem.¹⁴

Kedua, mekanisme immutability pada blockchain mendukung prinsip integritas data yang menjadi kewajiban pengendali data pribadi dalam Pasal 20 huruf c UU PDP, yaitu memastikan bahwa data pribadi akurat, lengkap, dan tidak dapat dimanipulasi. Ketika transaksi telah tercatat dalam blok, pencatatan tersebut tidak dapat diubah, sehingga mencegah praktik manipulasi data transaksi nasabah yang selama ini menjadi salah satu sumber fraud di sektor keuangan. Ketiga, penggunaan kriptografi kunci publik meningkatkan standar keamanan autentikasi pengguna. Berbeda dengan model tradisional perbankan yang mengandalkan OTP, PIN, dan password yang tersimpan di server pusat, blockchain bekerja dengan private key yang hanya dimiliki oleh pengguna. Hal ini sejalan dengan prinsip

¹¹ Fadhillah, A., Asikin, Z., & Parman, L. (2019). Prinsip Mengenal Nasabah (Know Your Customer Principle) Oleh Bank Dalam Pencegahan Tindak Pidana Pencucian Uang. *Media Bina Ilmiah*, 13(10), 1727-1738.

¹² Watkat, F. X., Ingratubun, M. T., & Ingsaputro, M. H. (2023). Pencegahan Tindak Pidana Pencucian Uang Melalui Penerapan Prinsip Customers Due Diligence Oleh Lembaga Perbankan Di Indonesia. *Jurnal Hukum Ius Publicum*, 4(2), 134-162.

¹³ Handoko, R. M., Trisna, B. A. A., Pratama, R. D., & Parhusip, J. (2024). Implementasi Blockchain untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik Dan Informatika*, 4(2), 64-74.

¹⁴ Martinelli, I., Tsabita, N. M., Putri, A. F. E., & Novela, D. (2024). Legalitas dan Efektivitas Penggunaan Teknologi Blockchain Terhadap Smart Contract Pada Perjanjian Bisnis di Masa Depan. *UNES Law Review*, 6(4), 10761-10776.

keamanan data sebagaimana diatur dalam Pasal 35 UU PDP, yang mengharuskan pengendali data menerapkan langkah keamanan teknis untuk mencegah akses tidak sah. Dengan verifikasi berbasis matematis, risiko pembobolan akibat pencurian OTP atau peretasan server menjadi jauh lebih kecil.¹⁵

blockchain menyediakan transparansi dan auditability, yang secara langsung mendukung kewajiban pencegahan pencucian uang dan pendanaan terorisme sebagaimana diatur dalam Peraturan Bank Indonesia Nomor 19/10/PBI/2017 tentang APU-PPT serta POJK Nomor 12/POJK.01/2017. Melalui pencatatan transaksi yang tidak dapat diubah dan dapat ditelusuri, fintech dapat memantau transaksi mencurigakan secara real-time, dan otoritas dapat menelusuri alur transaksi tanpa hambatan manipulasi data internal. Dengan demikian, blockchain memperkuat efektivitas Customer Due Diligence (CDD) tanpa menambah beban penyimpanan data sensitif secara berlebihan.¹⁶

Meskipun blockchain aman terhadap manipulasi, sistem ini tetap rentan terhadap risiko kehilangan atau pencurian kunci privat. Jika kunci privat pemilik data dicuri atau hilang, maka data dan aset digital dapat berpindah tangan tanpa mekanisme pemulihan seperti yang diatur pada sistem keuangan tradisional. Kondisi ini bertentangan dengan prinsip keamanan dan mitigasi risiko dalam Pasal 46 PP 71/2019, yang mewajibkan PSE menyediakan mekanisme pemulihan bila terjadi insiden keamanan. Dalam blockchain, pemulihan tidak mungkin dilakukan tanpa akses ke kunci privat, sehingga pengguna menanggung risiko penuh. blockchain publik bersifat terbuka dan dapat diakses semua node, sehingga berpotensi menimbulkan risiko *re-identification* terhadap data transaksi walaupun data tersaji dalam bentuk pseudonim. Hal ini berpotensi melanggar prinsip pembatasan tujuan dan minimalisasi data dalam Pasal 22 dan 23 UU PDP, karena aktivitas transaksi yang terus-menerus dapat dihubungkan kembali dengan identitas pengguna meskipun nama tidak disimpan secara langsung.¹⁷

blockchain memiliki masalah skalabilitas dan efisiensi, di mana proses validasi transaksi membutuhkan kapasitas besar dan waktu pemrosesan lebih lama dibanding sistem terpusat. Bagi PSE fintech yang wajib menjamin kecepatan layanan dan ketersediaan sistem sebagaimana diatur dalam Pasal 14 PP 71/2019, teknologi blockchain tertentu dapat menimbulkan hambatan operasional bila diterapkan sebagai penyimpanan utama data pengguna, karena keterbatasan legal dan teknis, blockchain tidak dapat sepenuhnya menggantikan sistem penyimpanan tradisional. Fintech tetap harus menyimpan data pribadi sensitif seperti KTP, biometrik, dan data CDD dalam server yang memenuhi kewajiban tata kelola data sesuai POJK APU-PPT dan Pasal 39–44 UU PDP tentang kewajiban pengendali dan prosesor data pribadi. Artinya, risiko kebocoran data tidak dapat sepenuhnya dieliminasi meskipun blockchain diterapkan.¹⁸

Kepatuhan Sistem Fintech Berbasis Blockchain Terhadap UU PDP & UU ITE di Indonesia.

Kepatuhan sistem fintech berbasis blockchain terhadap Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya (UU ITE), terakhir diubah melalui UU No. 1 Tahun 2024 menjadi aspek krusial mengingat karakteristik teknologi blockchain yang beroperasi secara immutable, transparan, dan desentralisasi. Dalam operasi *blockchain* tidak ada entitas tunggal yang mengendalikan seluruh proses dari awal transaksi sampai pencatatan. Pada pasal 20 UU PDP menjelaskan bahwa kewajiban bagi

¹⁵ Hasan, S. A., Al-Zahra, W. N., Auralia, A. S., Maharani, D. A., & Hidayatullah, R. (2024). Implementasi teknologi blockchain dalam pengamanan sistem keuangan pada perguruan tinggi: Implementation of blockchain technology in securing financial systems in higher education. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, 3(1), 11-18.

¹⁶ Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. *Jurnal USM Law Review*, 7(1), 333-347.

¹⁷ Wardhono, R. D. T. K., Badrawani, W., Deviana, A., Pramudyastuti, M., & Shalehanti, N. (2024). *Pelindungan Data Pribadi Di Bank Indonesia Dan Lembaga Jasa Keuangan: Rekomendasi Kebijakan Dan Teknis Pengaturan* (No. WP/16/2024).

¹⁸ Handoko, R. M., Trisna, B. A. A., Pratama, R. D., & Parhusip, J. (2024). Implementasi Blockchain untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik Dan Informatika*, 4(2), 64-74.

Pengendali Data Pribadi dan Prosesor Data Pribadi untuk memastikan pemrosesan data dilakukan secara sah, proporsional, terbatas pada tujuan tertentu, pada pasal 5-8 juga mengamanatkan bahwa subjek data pribadi memiliki hak seperti hak akses, koreksi, hingga penghapusan data. Namun, dalam arsitektur blockchain, pencatatan transaksi bersifat permanen dan tidak dapat dihapus menimbulkan konflik langsung dengan kewajiban pengendali data untuk memenuhi hak subjek data pribadi tersebut. Karena setiap data yang sudah tercatat pada rantai blok tidak dapat dimodifikasi atau dihapus.¹⁹ sistem fintech berbasis blockchain harus merancang model pemrosesan data yang mencegah data pribadi ditempatkan langsung pada ledger. Oleh karena itu, pemenuhan UU PDP di sektor ini tidak dapat dilakukan tanpa pendekatan arsitektur yang secara teknis menghindari penyimpanan informasi identitas di dalam block, melainkan memanfaatkan penyimpanan off-chain yang dapat dihapus atau dimodifikasi ketika dibutuhkan.²⁰

Selain itu, UU PDP mewajibkan adanya identifikasi jelas mengenai siapa yang bertindak sebagai Pengendali Data, sedangkan pada blockchain publik, node dijalankan oleh berbagai pihak yang mungkin tidak berada dalam yurisdiksi Indonesia. Dalam konteks fintech yang tunduk pada pengawasan Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) praktik ini tidak dapat diterima, sebab penyelenggara layanan keuangan wajib memiliki entitas yang dapat dimintai pertanggungjawaban. Karena itu, fintech yang memanfaatkan blockchain cenderung wajib menggunakan model permission blockchain atau blockchain privat, di mana penyelenggara layanan keuangan tetap menjadi Pengendali Data, sehingga ketentuan Pasal 4–20 UU PDP mengenai prinsip perlindungan data dapat dipenuhi. Pendekatan ini selaras dengan ketentuan POJK No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital dan POJK No. 77/POJK.01/2016, yang menempatkan penyelenggara sebagai pihak yang bertanggung jawab atas keamanan sistem, perlindungan konsumen, dan manajemen risiko operasional termasuk risiko keamanan data.²¹

Kepatuhan terhadap UU ITE, khususnya terkait keabsahan dokumen elektronik, keamanan sistem elektronik, dan kewajiban penyelenggara juga menjadi bagian penting. UU ITE dan PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) pada pasal 22 menjelaskan bahwa setiap Penyelenggara Sistem Elektronik (PSE) untuk wajib menyediakan keamanan yang memadai, memiliki prosedur audit, menyimpan rekam jejak transaksi, serta memastikan sistem dapat diakses oleh aparat penegak hukum ketika diperlukan. Blockchain memang menyediakan audit trail secara real time. namun, informasi tersebut belum tentu sesuai standar yang dapat digunakan dalam pembuktian formal jika data pribadi tidak dikelola dengan benar. Lebih jauh, PP 71/2019 juga mengatur mengenai penempatan dan transfer data lintas negara yang mensyaratkan adanya jaminan efektivitas pengawasan. Hal ini menjadi perhatian serius mengingat node blockchain kerap berada di berbagai wilayah dunia, sehingga fintech wajib memastikan bahwa pemrosesan data pribadi tidak secara otomatis mengalir ke node asing tanpa pengendalian hukum yang memadai. Pada sektor privat, kewajiban pendaftaran PSE berdasarkan Permen Kominfo No. 5 Tahun 2020 jo. Permen 10 Tahun 2021 juga menempatkan fintech berbasis blockchain dalam kewajiban menyerahkan akses sistem ketika terdapat permintaan yang sah menurut hukum.²²

Untuk mengatasi konflik teknis-hukum antara sifat immutable blockchain dan hak penghapusan data, model pemrosesan data yang dianjurkan adalah menggunakan arsitektur hybrid, yaitu menempatkan identitas atau data sensitif di off-chain storage yang terenkripsi, sementara blockchain hanya memuat hash yang tidak dapat mengidentifikasi individu. Ketika subjek data mengajukan

¹⁹ Harmen, H., Surbakti, O. M. B., Reynaldi, F. F., & Damanik, A. P. J. (2024). Peran Regulasi Cryptocurrency Terhadap Perkembangan Fintech Di Indonesia: Analisis Dari Sudut Pandang Hukum Bisnis. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, 4(1), 58-68.

²⁰ Maulana, M. R., Firdaus, M. R., Firdaus, M. H., Aziz, H. A., & Pratama, A. P. Penggunaan Teknologi Blockchain untuk Keamanan dan Efisiensi Sistem Fintech di Era Big Data.

²¹ Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. *Jurnal USM Law Review*, 7(1), 333-347.

²² Sahril, I., & Atmadja, D. A. W. (2025). Perlindungan Data Pribadi Konsumen, Dokumen dan Tanda Tangan Elektronik yang Dipergunakan oleh Pihak Ketiga dalam Transaksi E-Commerce. *CENDEKIA: Jurnal Penelitian Dan Pengkajian Ilmiah*, 2(2), 173-189.

permintaan penghapusan, pengendali cukup menghapus data di off-chain sehingga hash yang tersisa di blockchain tidak lagi memiliki makna personal. Beberapa praktik global juga mengizinkan pendekatan *crypto-shredding*, yaitu penghapusan kunci enkripsi sehingga data tidak dapat dipulihkan meskipun masih tersimpan dalam bentuk ciphertext. Pendekatan ini dinilai memenuhi prinsip efektivitas penghapusan pada UU PDP. Selain itu, penyelenggara fintech perlu menyusun Data Protection Impact Assessment (DPIA), menerapkan *privacy by design*, serta memiliki Standard Operating Procedure (SOP) untuk pemenuhan hak-hak subjek data.²³

Dengan demikian, kepatuhan sistem fintech berbasis blockchain terhadap UU PDP & UU ITE sangat bergantung pada desain arsitektur sistem, tata kelola data, serta mekanisme operasional yang memastikan bahwa immutability blockchain tidak menghambat terlaksananya kewajiban hukum. Sistem yang dirancang dengan meminimalkan data pribadi di blockchain, penempatan data sensitif di wilayah Indonesia atau setidaknya pada entitas yang diawasi, audit keamanan smart contract, serta pendaftaran resmi sebagai PSE dan kepatuhan terhadap regulasi sektor keuangan, merupakan prasyarat utama agar penggunaan teknologi blockchain dalam fintech dapat dinilai sejalan dengan kerangka hukum Indonesia. Dengan implementasi pendekatan desain yang tepat dan tata kelola yang kuat, penggunaan blockchain dalam sektor fintech tetap dapat memenuhi seluruh ketentuan perundang-undangan yang berlaku, meskipun karakter teknologinya pada dasarnya menantang beberapa prinsip mendasar perlindungan data.²⁴

SIMPULAN

Pada zaman yang serba digital seperti sekarang menyajikan kemudahan untuk memenuhi seluruh kebutuhan hidup, semua dapat kita dapatkan hanya lewat smartphone seperti membeli barang, kuota internet, token listrik, dan tiket wisata. Kita tidak perlu repot untuk datang ke toko dan membawa uang banyak karena pembayaran dapat kita lakukan dengan m-banking atau e wallet. Namun, perkembangan teknologi bagaikan pisau bermata dua yang dapat memberikan ancaman dibalik kemudahan yang diberikan. Salah satu contoh ancaman yang mengancam pengguna financial technology adalah pencurian data pribadi. Maka dari itu diperlukan suatu sistem penyimpanan data yang aman dan tidak mudah diretas, penulis melihat potensi teknologi blockchain untuk diterapkan pada teknologi financial technology, karena blockchain bersifat desentralisasi, transparan, dan immutable. Namun, kekosongan hukum yang mengatur terkait blockchain masih menjadi hambatan dalam penerapannya.

SARAN

Pemerintah perlu memperkuat regulasi dan pedoman teknis terkait penerapan blockchain dalam layanan fintech agar tercipta kepastian hukum serta standar keamanan yang seragam, sementara penyelenggara fintech harus meningkatkan kompetensi sumber daya manusia dan infrastruktur teknologi untuk memastikan integrasi blockchain berjalan optimal. Selain itu, kolaborasi antara regulator, industri, dan akademisi perlu diperkuat guna mengembangkan standar keamanan, mekanisme audit, serta model implementasi yang efektif dalam mencegah kebocoran data pribadi. Edukasi kepada pengguna layanan fintech juga penting agar masyarakat memahami cara kerja blockchain dan pentingnya menjaga data pribadinya, yang selanjutnya harus didukung oleh pengembangan infrastruktur keamanan digital nasional yang mampu menjamin keamanan, interoperabilitas, dan keandalan sistem.

²³ Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, 2(1), 55-68.

²⁴ Megawati, L., Wiharna, C., & Hasanudin, A. (2023). Peran Teknologi Blockchain Dalam Meningkatkan Keamanan Dan Kepastian Hukum Dalam Transaksi Kontrak Di Indonesia. *Jurnal Hukum Mimbar Justitia*, 9(2), 410-435.

REFERENSI

- Bakri, A. A., Hasanah, N., & Lasmiatun, K. M. T. (2024). *Financial technology innovation and banking industry transformation: A literature study on financial markets*. *Multifinance*, 1(3), 230–238.
- Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). *Perlindungan hukum terhadap keamanan data konsumen financial technology di Indonesia*. *Refleksi Hukum: Jurnal Ilmu Hukum*, 3(2), 145–160.
- Fadhillah, A., Asikin, Z., & Parman, L. (2019). *Prinsip mengenal nasabah (Know Your Customer Principle) oleh bank dalam pencegahan tindak pidana pencucian uang*. *Media Bina Ilmiah*, 13(10), 1727–1738.
- Handoko, R. M., Trisna, B. A. A., Pratama, R. D., & Parhusip, J. (2024). *Implementasi blockchain untuk keamanan sistem pembayaran digital dan optimasi transaksi keuangan (Studi kasus industri fintech di Indonesia)*. *Teknik: Jurnal Ilmu Teknik dan Informatika*, 4(2), 64–74.
- Harmen, H., Surbakti, O. M. B., Reynaldi, F. F., & Damanik, A. P. J. (2024). *Peran regulasi cryptocurrency terhadap perkembangan fintech di Indonesia: Analisis dari sudut pandang hukum bisnis*. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, 4(1), 58–68.
- Hasan, S. A., Al-Zahra, W. N., Auralia, A. S., Maharani, D. A., & Hidayatullah, R. (2024). *Implementasi teknologi blockchain dalam pengamanan sistem keuangan pada perguruan tinggi*. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, 3(1), 11–18.
- Kurniati, R. R., & Junaida, D. (2019). *Pengaruh e-commerce terhadap keputusan pembelian pada belanja online Shopee (Studi pada konsumen mahasiswa Universitas Islam Malang)*. *JIAGABI (Jurnal Ilmu Administrasi Niaga/Bisnis)*, 8(3), 154–162.
- Maharani, R., & Prakoso, A. L. (2024). *Perlindungan data pribadi konsumen oleh penyelenggara sistem elektronik dalam transaksi digital*. *Jurnal USM Law Review*, 7(1), 333–347.
- Martinelli, I., Tsabita, N. M., Putri, A. F. E., & Novela, D. (2024). *Legalitas dan efektivitas penggunaan teknologi blockchain terhadap smart contract pada perjanjian bisnis di masa depan*. *UNES Law Review*, 6(4), 10761–10776.
- Maulana, M. R., Firdaus, M. R., Firdaus, M. H., Aziz, H. A., & Pratama, A. P. *Penggunaan teknologi blockchain untuk keamanan dan efisiensi sistem fintech di era big data*. (Jurnal tidak tercantum lengkap dalam footnote).
- Megawati, L., Wiharma, C., & Hasanudin, A. (2023). *Peran teknologi blockchain dalam meningkatkan keamanan dan kepastian hukum dalam transaksi kontrak di Indonesia*. *Jurnal Hukum Mimbar Justitia*, 9(2), 410–435.
- Pakpahan, J. M. (2024). *Kesadaran urgensi peran pengendali dan prosesor data pribadi berdasarkan UU PDP 2022*. *Jurnal Hukum To-Ra*, 10(1), 119–137.
- Palinggi, S., & Limbongan, E. C. (2020). *Pengaruh internet terhadap industri e-commerce dan regulasi perlindungan data pribadi pelanggan di Indonesia*. *Semnas Ristek*, 4(1).
- Purwanto, H., Yandri, D., & Yoga, M. P. (2022). *Perkembangan dan dampak financial technology (fintech) terhadap perilaku manajemen keuangan masyarakat*. *Kompleksitas: Jurnal Ilmiah Manajemen, Organisasi dan Bisnis*, 11(1), 80–91.
- Sahril, I., & Atmadja, D. A. W. (2025). *Perlindungan data pribadi konsumen, dokumen, dan tanda tangan elektronik oleh pihak ketiga dalam transaksi e-commerce*. *CENDEKIA: Jurnal Penelitian dan Pengkajian Ilmiah*, 2(2), 173–189.
- Setiawan, H. B., & Najicha, F. U. (2022). *Perlindungan data pribadi warga negara Indonesia terkait kebocoran data*. *Jurnal Kewarganegaraan*, 6(1), 976–982.
- Suryawijaya, T. W. E. (2023). *Memperkuat keamanan data melalui teknologi blockchain: Implementasi sukses dalam transformasi digital di Indonesia*. *Jurnal Studi Kebijakan Publik*, 2(1), 55–68.
- Utomo, S., Safuan, S., & Alhabsy, M. A. (2023). *Implementasi kebijakan penggunaan QRIS terhadap praktik UMKM sebagai upaya percepatan pertumbuhan ekonomi digital*. (Jurnal tidak disebutkan lengkap di footnote).

- Watkat, F. X., Ingratubun, M. T., & Ingsaputro, M. H. (2023). *Pencegahan tindak pidana pencucian uang melalui penerapan prinsip customer due diligence oleh lembaga perbankan di Indonesia*. Jurnal Hukum Ius Publicum, 4(2), 134–162.
- Wardhono, R. D. T. K., Badrawani, W., Deviana, A., Pramudyastuti, M., & Shalehanti, N. (2024). *Pelindungan data pribadi di Bank Indonesia dan lembaga jasa keuangan: Rekomendasi kebijakan dan teknis pengaturan*. Working Paper Bank Indonesia, WP/16/2024.
- Zainuddin, M., & Karina, A. D. (2023). *Penggunaan metode yuridis normatif dalam membuktikan kebenaran pada penelitian hukum*. Smart Law Journal, 2(2), 114–123.