

**REKONSTRUKSI PEMBUKTIAN PERKARA PIDANA
PADA UU NO. 20 TAHUN 2025: IMPLEMENTASI
BLOCKCHAIN PADA MEKANISME CHAIN OF CUSTODY
DAN AUTENTIKASI BUKTI DIGITAL**

**Muhammad Farid Akbar¹, Dhutra Aditya Pratama², Rashan Devano³,
Priya Rajata Sinaga⁴
Universitas Sahid**

Email: [¹2024510017@usahid.ac.id](mailto:2024510017@usahid.ac.id), [²2024510035@usahid.ac.id](mailto:2024510035@usahid.ac.id), [³2024510020@usahid.ac.id](mailto:2024510020@usahid.ac.id),
[⁴2024510013@usahid.ac.id](mailto:2024510013@usahid.ac.id)

ABSTRAK

Pengesahan Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP Baru memperketat syarat autentikasi alat bukti elektronik melalui Pasal 235, namun praktik chain of custody di Indonesia masih bertumpu pada dokumentasi manual yang rentan terhadap kesalahan administratif dan rekayasa tanpa mekanisme verifikasi independen. Penelitian ini bertujuan merumuskan model chain of custody berbasis blockchain yang memenuhi syarat pengeledahan dan penyitaan (Pasal 113, 116, 119, 124), merekonstruksi proses pembuktian dari tahap penyidikan hingga persidangan untuk menjamin integritas dan ketelusuran bukti digital, serta menguji implikasi model terhadap exclusionary rule dan kepastian hukum berdasarkan Pasal 235. Penelitian hukum normatif ini menggunakan pendekatan perundang-undangan, konseptual, dan analitis terhadap bahan hukum primer, sekunder, dan tersier. Hasil penelitian menunjukkan bahwa blockchain secara teknis memenuhi empat dari lima parameter kepatuhan terhadap KUHAP Baru, sementara keabsahan perolehan awal bukti tidak pernah dapat dijamin secara otomatis oleh teknologi. Model rekonstruksi mengadopsi arsitektur hybrid on-chain/off-chain empat tahap yang mengaitkan entri awal ledger dengan nomor izin pengeledahan atau penyitaan dari pengadilan. Blockchain tidak dapat memulihkan cacat prosedural pada tahap perolehan bukti karena integritas kriptografis dan keabsahan perolehan bekerja pada tataran independen. Penelitian ini menyimpulkan bahwa blockchain memperkuat autentisitas dan ketelusuran bukti digital, namun memerlukan peraturan pelaksana yang secara eksplisit mengaitkan entri ledger dengan otorisasi yudisial agar bukti tersebut dapat diakui keabsahannya di persidangan.

Kata Kunci: Bukti Digital, Blockchain, Chain of Custody, KUHAP Baru, Exclusionary Rule.

ABSTRACT

The enactment of Law No. 20 of 2025 on the New Criminal Procedure Code (KUHP Baru) tightens the authentication requirements for electronic evidence under Article 235, yet Indonesia's chain-of-custody practice still relies on manual documentation vulnerable to administrative error and falsification, with no independent verification mechanism. This study aims to formulate a blockchain-based chain-of-custody model satisfying search-and-seizure requirements (Articles 113, 116, 119, 124), reconstruct the evidentiary process from investigation to trial to guarantee integrity and traceability of digital evidence, and examine the model's implications for the exclusionary rule doctrine and legal certainty under Article 235. This normative legal research applies statute, conceptual, and analytical approaches to primary, secondary, and tertiary legal materials. The results show that blockchain technically satisfies four of five compliance parameters mapped against KUHP Baru, while the lawfulness of evidence's initial acquisition can never be guaranteed automatically by technology. The reconstructed model adopts a four-stage hybrid on-chain/off-chain architecture linking the ledger's genesis entry to the court's search or seizure authorization number. Blockchain cannot cure procedural defects in acquisition, since cryptographic integrity and acquisition legality operate on independent planes. The study concludes that blockchain strengthens authenticity and traceability of digital evidence but requires implementing regulations explicitly linking ledger entries to judicial authorization before such evidence can be recognized as valid at trial.

Keywords: *Blockchain, Digital Evidence, Chain of Custody, New Criminal Procedure Code, Exclusionary Rule.*

PENDAHULUAN

Salah satu perubahan paling signifikan terletak pada Pasal 235 yang memperkenalkan jenis alat bukti baru berupa bukti elektronik dan pengamatan hakim, sekaligus mensyaratkan bahwa setiap alat bukti harus dapat diautentikasi dan diperoleh secara tidak melawan hukum. Konsekuensi dari ketentuan ini diatur tegas dalam Pasal 235 ayat (5), yang menyatakan bahwa alat bukti yang oleh hakim dinyatakan tidak autentik dan/atau diperoleh secara melawan hukum tidak dapat dipergunakan sebagai alat bukti dan tidak memiliki kekuatan pembuktian. Ketentuan ini menempatkan beban baru bagi penegak hukum, sebab tidak cukup lagi sekadar membawa suatu barang menjadi bukti, tetapi juga harus mampu menunjukkan rangkaian penguasaan (chain of custody) yang dapat dipertanggungjawabkan secara teknis maupun yuridis.

Perkembangan kejahatan di Indonesia semakin bertumpu pada jejak digital, mulai dari transaksi elektronik, percakapan pada aplikasi pesan instan, hingga rekaman pada sistem perbankan dan platform media sosial. Karakteristik bukti digital yang rentan terhadap penghapusan, penggantian, maupun kontaminasi data menjadikan mekanisme chain of custody konvensional, yang umumnya hanya bersandar pada berita acara manual dan keterangan saksi ahli, semakin sulit diandalkan untuk menjamin keaslian bukti sepanjang siklus penyidikan hingga persidangan. Praktik peradilan menunjukkan bahwa keabsahan bukti elektronik kerap diperdebatkan bukan karena isi buktinya, melainkan karena ketidakjelasan rantai penguasaannya sejak disita hingga diajukan di muka persidangan. KUHP Baru, melalui Pasal 113, 116, 119, dan 124, memang telah memperketat syarat formal penggeledahan dan penyitaan dengan mewajibkan izin ketua pengadilan negeri serta batas waktu persetujuan paling lama 2x24 jam dalam keadaan mendesak, namun ketentuan tersebut belum menjawab persoalan teknis mengenai bagaimana integritas barang bukti digital itu sendiri dapat dijamin secara matematis sepanjang proses pengalihan penguasaan antarinstansi penegak hukum.

Kajian mengenai pemanfaatan teknologi blockchain untuk menjamin integritas chain of custody bukti digital telah berkembang pesat dalam literatur forensik digital internasional. Lone dan Mir (2017, 2019) memperkenalkan model Forensic-Chain, sebuah rancang bangun

berbasis Ethereum dan Hyperledger Composer yang mencatat hash setiap bukti digital beserta rangkaian pengalihan penguasaannya ke dalam distributed ledger sehingga setiap penyimpangan dapat terdeteksi secara otomatis. Bonomi, Casini, dan Ciccotelli (2020) mengusulkan arsitektur B-CoC yang menambahkan mekanisme kontrol akses berbasis kriptografi untuk memastikan hanya pihak yang berwenang yang dapat mengakses maupun memindahkan kepemilikan bukti dalam ledger. Patil, Kohli, Puri, dan Puri (2024) melalui telaah literatur sistematis menunjukkan bahwa penerapan blockchain pada chain of custody secara konsisten meningkatkan auditabilitas dan resistensi terhadap manipulasi data forensik, sementara Onyeashie, Leimich, McKeown, dan Russell (2024) dalam analisis bibliometrik menyimpulkan bahwa tren penelitian pada bidang ini masih didominasi pendekatan teknis-komputasional dan belum banyak menyentuh dimensi kepatuhan terhadap hukum acara pidana suatu negara tertentu.

Kajian terdahulu lebih banyak terfokus pada status normatif bukti elektronik dan belum menyentuh mekanisme teknis penjaminan integritasnya. Ramiyanto (2017) menegaskan bahwa bukti elektronik telah lama diakui sebagai alat bukti yang sah dalam hukum acara pidana melalui Undang-Undang Informasi dan Transaksi Elektronik, namun penerapannya di persidangan masih bergantung pada keterangan ahli untuk membuktikan keasliannya. Lakada, Antouw, dan Bawole (2024) mengkaji perkembangan pengaturan alat bukti elektronik dalam konteks cyber crime dan menemukan bahwa KUHAP lama tidak memberikan kerangka prosedural yang baku mengenai bagaimana integritas bukti digital harus dijaga sejak penyitaan. Kajian yang lebih baru mengenai forensik digital berbasis blockchain pada kasus aset kripto di Indonesia juga menunjukkan adanya kesenjangan antara kapasitas teknis forensik blockchain dengan kebutuhan penegakan hukum serta kerangka regulasi yang masih belum memadai, sebagaimana hukum acara pidana yang berlaku belum mengatur standar baku autentikasi bukti berbasis teknologi distributed ledger. Fenomena kerentanan sistem hukum terhadap serangan siber tidak hanya terbatas pada integritas barang bukti, tetapi juga pada keselamatan subjek hukum yang melaporkan tindak pidana. Kasus Eko Sulisty (2023), yang mengalami serangan siber masif setelah melaporkan dugaan korupsi, mengungkapkan bahwa sistem perlindungan hukum konvensional gagal mengantisipasi ancaman digital terhadap whistleblower (Fahririn et al., 2026). Hal ini memperkuat urgensi pengembangan mekanisme autentikasi bukti digital yang tidak hanya menjamin integritas data, tetapi juga melindungi kerahasiaan identitas pelapor melalui teknologi kriptografi.

Berdasarkan uraian state of the art tersebut, dapat diidentifikasi dua kecenderungan dalam literatur yang ada. Pertama, kajian teknis-komputasional mengenai blockchain chain of custody umumnya dirancang secara generik tanpa dikaitkan langsung dengan syarat formil penggeledahan, penyitaan, dan autentikasi yang berlaku pada suatu sistem hukum acara pidana tertentu. Kedua, kajian hukum pembuktian di Indonesia umumnya membahas status bukti elektronik secara normatif tanpa merumuskan model teknis operasional yang dapat menjawab kebutuhan autentikasi sebagaimana dimandatkan Pasal 235 KUHAP Baru. Kekosongan inilah yang menjadi kebaruan ilmiah artikel ini, yaitu merumuskan dan menguji kesesuaian model chain of custody berbasis blockchain terhadap rezim hukum acara pidana yang sama sekali baru, mengingat KUHAP Baru baru efektif berlaku sejak 2 Januari 2026 sehingga belum tersedia kajian akademik yang secara spesifik menjembatani arsitektur teknis blockchain dengan syarat Pasal 113, 116, 119, 124, dan 235 KUHAP Baru, sekaligus menguji batas berlakunya doktrin exclusionary rule terhadap bukti yang telah terverifikasi secara kriptografis.

Berdasarkan latar belakang dan kebaruan ilmiah tersebut, penelitian ini merumuskan tiga permasalahan sebagai berikut.

1. Bagaimana mekanisme chain of custody barang bukti digital menggunakan teknologi blockchain dapat diimplementasikan untuk memenuhi standar penggeledahan dan penyitaan dalam KUHAP Baru?
2. Bagaimana rekonstruksi sistem pembuktian perkara pidana melalui implementasi teknologi blockchain guna menjamin integritas, transparansi, dan ketelusuran (traceability) barang bukti digital dari tahap penyidikan hingga persidangan?
3. Bagaimana implikasi penerapan teknologi blockchain dalam autentikasi bukti digital terhadap prinsip exclusionary rule dan kepastian hukum dalam sistem pembuktian perkara pidana berdasarkan UU No. 20 Tahun 2025?

Berdasarkan rumusan masalah tersebut, artikel ini ditujukan untuk mencapai tiga sasaran utama. Pertama, terciptanya kepastian hukum yang lebih tinggi, dalam arti hakim tidak lagi ragu menerima bukti digital karena integritasnya telah terverifikasi secara matematis melalui kriptografi, bukan sekadar bersandar pada keterangan lisan saksi ahli. Kedua, minimalisasi fabricated evidence, yaitu menutup peluang pemalsuan, penggantian, atau kontaminasi bukti digital oleh oknum penegak hukum maupun pihak ketiga karena setiap akses dan modifikasi terhadap bukti tercatat secara permanen pada distributed ledger. Ketiga, memastikan bahwa pemanfaatan teknologi informasi dalam kerangka KUHAP Baru dapat memberikan kebenaran materiil yang lebih terjamin tanpa mengabaikan asas due process of law, mengingat kepastian hukum yang dibangun di atas bukti yang tidak sah perolehannya tetap tidak memiliki legitimasi yuridis.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif (legal normative research), yaitu penelitian yang menempatkan hukum sebagai sistem norma mengenai prinsip, asas, kaidah, dan aturan perundang-undangan, putusan pengadilan, dan doktrin yang koheren. Objek utama penelitian adalah Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, khususnya Pasal 113, 116, 119, 124, 235, dan 241, yang dikaji secara sistematis untuk merumuskan model chain of custody berbasis blockchain yang sesuai dengan syarat normatifnya.

Penelitian ini menggunakan tiga pendekatan. Pertama, pendekatan perundang-undangan (statute approach) digunakan untuk menelaah keterkaitan antarpasal dalam KUHAP Baru yang mengatur upaya paksa penggeledahan dan penyitaan, jenis alat bukti, serta syarat autentikasinya. Kedua, pendekatan konseptual (conceptual approach) digunakan untuk membangun konstruksi teknis chain of custody berbasis blockchain dengan merujuk pada konsep hash kriptografis, distributed ledger, dan smart contract sebagaimana dikembangkan dalam literatur forensik digital. Ketiga, pendekatan analitis (analytical approach) digunakan untuk menguji konsistensi makna frasa "autentik" dan "diperoleh secara tidak melawan hukum" dalam Pasal 235 terhadap karakteristik teknis pembuktian.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, yaitu UU No. 20 Tahun 2025 tentang KUHAP beserta peraturan terkait; bahan hukum sekunder, berupa jurnal ilmiah, hasil penelitian, dan kajian doktrinal mengenai blockchain dan hukum pembuktian; serta bahan hukum tersier, berupa kamus hukum dan dokumen resmi lembaga peradilan. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research) dengan menelusuri basis data jurnal internasional dan nasional, naskah akademik, serta dokumen resmi penyusunan KUHAP Baru. Seluruh bahan hukum yang terkumpul kemudian dianalisis menggunakan metode analisis kualitatif yang bersifat deskriptif-analitis, yakni dengan menggambarkan ketentuan normatif yang berlaku, mengelaborasikannya dengan konsep teknis blockchain, dan menarik kesimpulan secara preskriptif mengenai kesesuaian

maupun ketidaksesuaian antara keduanya.

HASIL DAN PEMBAHASAN

A. Kesesuaian Mekanisme Chain of Custody Berbasis Blockchain dengan Standar Penggeledahan dan Penyitaan

Perkembangan teknologi informasi telah mengubah karakteristik alat bukti dalam proses peradilan pidana. Jika sebelumnya pembuktian lebih banyak bertumpu pada barang bukti fisik, saat ini bukti digital menjadi salah satu alat bukti yang semakin dominan dalam mengungkap tindak pidana. Berbeda dengan barang bukti konvensional, bukti digital memiliki karakteristik mudah disalin, dipindahkan, dimodifikasi, bahkan dihapus tanpa meninggalkan perubahan yang tampak secara kasat mata.¹ Oleh karena itu, proses penanganan bukti digital memerlukan mekanisme yang mampu menjamin keaslian, integritas, dan kesinambungan penguasaan barang bukti sejak pertama kali diperoleh hingga diajukan di persidangan. Mekanisme tersebut dikenal sebagai *chain of custody*.

Dalam konteks hukum acara pidana, *chain of custody* merupakan rangkaian dokumentasi yang mencatat setiap proses penanganan barang bukti, mulai dari pengumpulan, penyimpanan, pemeriksaan, pemindahan, hingga penyajiannya di persidangan. Dokumentasi tersebut memuat informasi mengenai waktu, identitas petugas, lokasi penyimpanan, serta tindakan yang dilakukan terhadap barang bukti. Pencatatan yang dilakukan secara berkesinambungan bertujuan untuk membuktikan bahwa barang bukti yang diajukan di persidangan merupakan barang bukti yang sama sebagaimana diperoleh pada saat penyidikan dan tidak mengalami perubahan selama proses penanganannya.² Dengan demikian, *chain of custody* berfungsi sebagai jaminan atas autentisitas dan integritas barang bukti digital sehingga dapat memenuhi syarat sebagai alat bukti yang sah.

Pemetaan terhadap Pasal 113, 116, 119, dan 124 KUHAP Baru menghasilkan kerangka acuan yang menjadi parameter kesesuaian suatu mekanisme teknologi dengan syarat sah penggeledahan dan penyitaan. Pasal 113 ayat (1) mewajibkan penyidik mengajukan permohonan izin penggeledahan kepada ketua pengadilan negeri sebelum tindakan dilakukan, sementara Pasal 113 ayat (4) memberikan pengecualian dalam keadaan mendesak, seperti tertangkap tangan atau berpotensi terjadi penghilangan barang bukti, dengan kewajiban memperoleh persetujuan ketua pengadilan negeri paling lama 2x24 jam setelah penggeledahan dilaksanakan. Apabila ketua pengadilan negeri menolak memberikan persetujuan tersebut, hasil penggeledahan tidak dapat dijadikan alat bukti. Ketentuan yang relatif sama berlaku bagi penyitaan dalam Pasal 119 ayat (1) dan Pasal 124, yang mensyaratkan izin ketua pengadilan negeri di tempat keberadaan benda yang akan disita, dengan kewajiban memuat jenis, jumlah, dan nilai barang serta alasan penyitaan dalam permohonan izin.

Implikasi yuridis dari kerangka tersebut bagi rancang bangun blockchain chain of custody adalah bahwa pencatatan hash dan metadata bukti digital ke dalam distributed ledger hanya layak dilakukan setelah, atau bersamaan dengan, terpenuhinya syarat formil penggeledahan/penyitaan di atas. Artinya, entri pertama (genesis entry) dalam ledger harus secara eksplisit menyertakan rujukan terhadap nomor izin atau penetapan persetujuan ketua

¹ Leny Megawati., Cecep Wiharna., Asep Hasanudin., "Peran Teknologi Blockchain dalam Meningkatkan Keamanan dan Kepastian Hukum dalam Transaksi Kontrak di Indonesia," Jurnal Hukum Mimbar Justitia Volume 9, No. 2 Edisi/Issue (2023): Halaman 412, <https://pdfs.semanticscholar.org/7951/dc82ee4abfa395674fcef1f0083aa5e9c8a7.pdf>.

² Kurnia Ramadhan, "Chain Of Custody berbasis Blockchain dalam Penanganan Bukti Digital," Hukumonline.com, 5 Agustus 2023, <https://www.hukumonline.com/berita/a/chain-of-custody-berbasis-blockchain-dalam-penanganan-bukti-digital-lt64ce49bc3bf67/?page=all> , diakses pada tanggal 28 Juni 2026.

pengadilan negeri, baik yang diterbitkan sebelum tindakan (skema normal Pasal 113 ayat 1 dan Pasal 119 ayat 1) maupun yang menyusul dalam keadaan mendesak (skema Pasal 113 ayat 4 dan 6). Tanpa keterkaitan eksplisit ini, ledger hanya akan mencatat integritas data secara teknis tetapi gagal merefleksikan keabsahan prosedural perolehannya, sehingga bukti tetap berisiko dikesampingkan meskipun chain of custody-nya terjaga sempurna secara kriptografis.

Untuk menguji apakah mekanisme blockchain yang dirumuskan benar-benar memenuhi syarat "dapat diautentikasi" dan "diperoleh secara tidak melawan hukum" sebagaimana dimandatkan Pasal 235 ayat (3) dan (5), penelitian ini menyusun matriks kepatuhan sebagaimana disajikan pada Tabel 1.

Tabel 1 Matriks Kepatuhan Mekanisme Chain of Custody Berbasis Blockchain terhadap Syarat KUHAP Baru

Tahapan Hukum Acara	Dasar Hukum (KUHP Baru)	Mekanisme Blockchain	Status Kepatuhan
Penggeledahan dengan izin	Pasal 113 ayat (1)	Nomor izin/penetapan ketua PN direkam sebagai entri awal ledger sebelum penggeledahan	Terpenuhi
Penggeledahan keadaan mendesak	Pasal 113 ayat (4) dan (6)	Entri awal ditandai status "sementara" hingga persetujuan ketua PN terunggah dalam 2x24 jam	Terpenuhi bersyarat
Penyitaan dengan izin	Pasal 119 ayat (1); Pasal 124	Nomor izin penyitaan dan lokasi benda direkam sebagai metadata wajib pada entri ledger	Terpenuhi
Autentikasi bukti elektronik	Pasal 235 ayat (1) huruf f; ayat (3)	Hash kriptografis (SHA-256) dicocokkan pada setiap tahap penyajian bukti	Terpenuhi
Keabsahan perolehan bukti	Pasal 235 ayat (4) dan (5)	Ledger hanya mencatat integritas pasca-perolehan, tidak menjamin keabsahan perolehan awal	Tidak terpenuhi otomatis

Tabel 1 menunjukkan bahwa empat dari lima tahapan dapat dipenuhi secara teknis oleh mekanisme blockchain, sementara satu tahapan, yaitu keabsahan perolehan awal bukti, tidak dapat dipenuhi secara otomatis oleh teknologi apa pun karena menyangkut penilaian yuridis terhadap proses sebelum data dimasukkan ke dalam sistem. Temuan ini konsisten dengan hasil penelitian Patil, Kohli, Puri, dan Puri (2024) yang menegaskan bahwa kontribusi utama blockchain dalam forensik digital terletak pada integritas pasca-akuisisi (post-acquisition integrity), bukan pada keabsahan proses akuisisi itu sendiri. Dengan demikian, kepatuhan teknis terhadap Pasal 235 ayat (3) hanya dapat tercapai penuh apabila diiringi kepatuhan prosedural terhadap Pasal 113, 116, 119, dan 124 sejak awal.

Dari sisi perlindungan hak konstitusional tersangka, khususnya hak atas privasi, penerapan blockchain chain of custody perlu dibatasi pada pencatatan metadata dan nilai hash, bukan konten substantif bukti digital itu sendiri. Pencantuman isi data pribadi secara penuh ke dalam ledger yang bersifat permanen dan tidak dapat dihapus (immutable) berpotensi melanggar prinsip pembatasan tujuan pengolahan data pribadi, mengingat data tersebut dapat tetap tersimpan meskipun perkara telah diputus bebas atau dihentikan. Oleh

karena itu, desain yang direkomendasikan dalam penelitian ini adalah arsitektur hybrid, yaitu menyimpan konten bukti digital pada repositori off-chain yang aman, sementara hash, stempel waktu, dan metadata rantai kepemilikan disimpan pada distributed ledger berjenis permissioned (bukan publik), sehingga akses hanya diberikan kepada pihak yang berwenang dalam proses peradilan pidana.

Berdasarkan temuan ini, penelitian merekomendasikan agar Mahkamah Agung atau Pemerintah menerbitkan regulasi pelaksana, baik dalam bentuk Peraturan Mahkamah Agung maupun Peraturan Pemerintah, yang secara eksplisit mengatur bahwa entri pertama pada distributed ledger bukti digital wajib mencantumkan rujukan terhadap izin atau penetapan persetujuan penggeledahan/penyitaan dari ketua pengadilan negeri, sebagai prasyarat normatif sebelum suatu mekanisme blockchain chain of custody dapat diakui keabsahannya dalam persidangan.

Dalam implementasinya, *blockchain* tidak digunakan untuk menyimpan keseluruhan isi barang bukti digital karena ukuran data yang relatif besar dan pertimbangan efisiensi penyimpanan. Sebaliknya, sistem *blockchain* menyimpan metadata berupa nilai hash, timestamp, identitas petugas yang menangani barang bukti, lokasi penyimpanan, serta riwayat setiap perpindahan atau tindakan terhadap barang bukti. Sementara itu, file asli tetap disimpan pada media penyimpanan yang aman (*off-chain storage*).³ Dengan mekanisme tersebut, setiap perubahan terhadap file asli akan menghasilkan nilai hash yang berbeda sehingga integritas barang bukti dapat diverifikasi setiap saat

Apabila dikaitkan dengan ketentuan dalam Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, penggunaan blockchain sebagai mekanisme *chain of custody* pada dasarnya tidak bertentangan dengan standar hukum yang berlaku. Pasal 235 ayat (3) mensyaratkan bahwa alat bukti elektronik harus dapat diautentikasi, sedangkan ayat (5) menghendaki agar alat bukti tersebut diperoleh melalui prosedur yang sah.⁴ Dalam konteks ini, *blockchain* bukan merupakan alat untuk memperoleh barang bukti, melainkan teknologi yang digunakan untuk menjamin bahwa barang bukti yang telah diperoleh secara sah tetap terpelihara integritas dan autentisitasnya selama proses penegakan hukum berlangsung.

Selain memenuhi persyaratan autentikasi, penerapan *blockchain* juga harus diselaraskan dengan ketentuan mengenai penggeledahan dan penyitaan sebagaimana diatur dalam Pasal 113, Pasal 116, Pasal 119, dan Pasal 124 Undang-Undang Nomor 20 Tahun 2025. Ketentuan tersebut pada dasarnya mengatur syarat formil mengenai kewenangan penyidik, izin pengadilan, pelaksanaan penggeledahan, tata cara penyitaan, serta batas waktu pelaporan dalam keadaan tertentu. *Blockchain* tidak mengubah prosedur tersebut karena teknologi ini baru digunakan setelah barang bukti diperoleh melalui mekanisme yang sesuai dengan hukum. Dengan demikian, penggunaan *blockchain* tidak dapat dijadikan dasar untuk mengesampingkan kewajiban memperoleh izin penggeledahan maupun penyitaan sebagaimana diatur dalam KUHAP.⁵

Di sisi lain, penggunaan *blockchain* juga perlu memperhatikan perlindungan hak konstitusional tersangka, khususnya hak atas privasi dan hak untuk memperoleh proses hukum yang adil (*due process of law*). Pemanfaatan *blockchain* tidak boleh dimaknai

³ Arif Putra Surya, Yudi Prayudi, "Implementasi Multi Smart Contract pada Bukti Digital dan Chain of Custody dalam Meningkatkan Keamanan dan Integritas Bukti Digital," *Justindo* Volume 6, No. 2, Issue (2021): Halaman 100, https://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/3945?utm_source=perplexity.

⁴ Indonesia, Undang-Undang Nomor 20 Tahun 2025 Tentang Kitab Undang-Undang Hukum Pidana, Pasal 235 ayat (3) dan ayat (5)

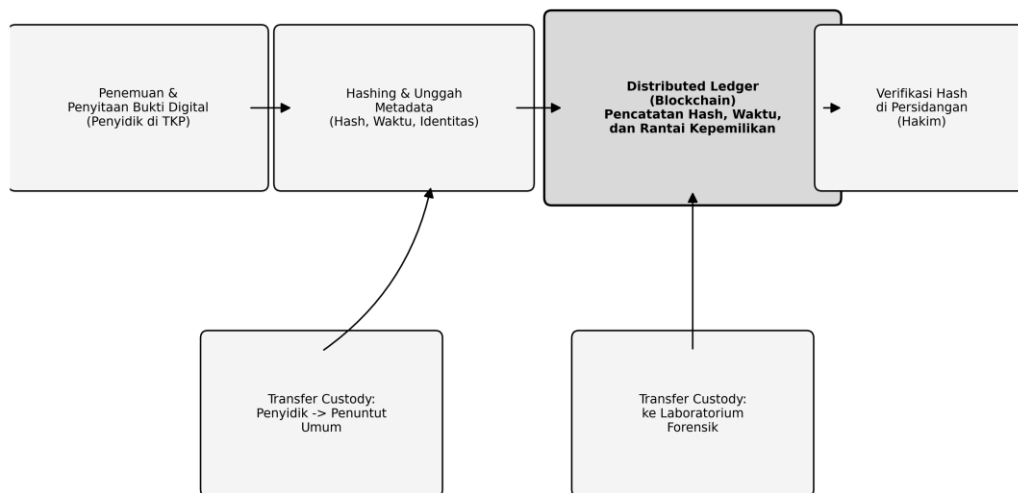
⁵ Indonesia, Undang-Undang Nomor 20 Tahun 2025 Tentang Kitab Undang-Undang Hukum Pidana, Pasal 113, Pasal 116, Pasal 119, dan Pasal 124

sebagai legitimasi bagi aparat penegak hukum untuk melakukan pengumpulan data secara berlebihan ataupun menyimpan informasi pribadi yang tidak berkaitan dengan tindak pidana yang sedang diselidiki. Oleh karena itu, penerapan *blockchain* sebaiknya hanya digunakan untuk mencatat metadata yang berkaitan dengan proses penanganan barang bukti, sedangkan isi data pribadi tetap dilindungi melalui mekanisme enkripsi dan pembatasan akses sesuai prinsip perlindungan data pribadi.

B. Rekonstruksi Sistem Pembuktian Berbasis Blockchain: Integrasi Model, Protokol, dan Traceability dari Penyidikan hingga Persidangan

Setidaknya tiga celah utama dapat diidentifikasi. Pertama, pencatatan penyitaan dan pengalihan penguasaan bukti digital pada praktik konvensional masih mengandalkan berita acara manual yang rawan kesalahan administratif maupun rekayasa tanggal. Kedua, tidak terdapat mekanisme verifikasi independen yang memungkinkan pihak di luar penyidik memastikan bahwa bukti yang diajukan di persidangan identik dengan yang disita di tempat kejadian perkara, sehingga keabsahannya semata-mata bergantung pada keterangan saksi ahli yang bersifat subjektif. Ketiga, pengalihan penguasaan dari penyidik ke penuntut umum maupun ke laboratorium forensik kerap tidak terdokumentasi secara real-time, menciptakan jeda waktu (*custody gap*) yang berpotensi dimanfaatkan untuk memalsukan atau mengganti bukti. Celah-celah inilah yang melatari kebutuhan terhadap rekonstruksi sistem pembuktian berbasis blockchain.

Berdasarkan pemetaan celah tersebut, penelitian ini merumuskan model rekonstruksi sistem pembuktian sebagaimana digambarkan pada Gambar 1, yang terdiri atas empat tahap utama: (1) penemuan dan penyitaan bukti digital oleh penyidik; (2) penghitungan nilai hash serta pengunggahan metadata ke distributed ledger; (3) pencatatan setiap transfer custody, baik kepada penuntut umum maupun laboratorium forensik, sebagai entri baru yang bersifat immutable pada ledger yang sama; dan (4) verifikasi hash secara mandiri oleh hakim pada tahap persidangan.



Catatan: setiap transfer custody dicatat sebagai entri baru yang immutable pada distributed ledger.

Gambar 1 Model Rekonstruksi Chain of Custody Bukti Digital Berbasis Blockchain

Pada tahap pertama, protokol teknis yang direkomendasikan adalah sebagai berikut. Penyidik, baik dari kepolisian, PPNS, maupun kejaksaan, menghitung nilai hash bukti digital menggunakan algoritma kriptografis standar (misalnya SHA-256) segera setelah bukti ditemukan dan sebelum dilakukan duplikasi data (forensic imaging). Nilai hash, stempel waktu, identitas penyidik, serta nomor izin penggeledahan/penyitaan kemudian diunggah sebagai entri pertama pada distributed ledger. Prosedur ini sejalan dengan rancangan Forensic-Chain yang dikembangkan Lone dan Mir (2019), yang menempatkan first responder sebagai pemicu awal pencatatan rantai kepemilikan bukti digital, namun dalam

konteks KUHAP Baru, prosedur tersebut perlu ditambahkan kewajiban mencantumkan rujukan izin pengadilan sebagai elemen metadata wajib, sebagaimana telah dijelaskan pada subbagian sebelumnya.

Pada tahap ketiga, setiap pergantian penanggung jawab barang bukti, baik dari penyidik kepada penuntut umum maupun kepada laboratorium forensik, direkam sebagai entri baru pada ledger yang memuat identitas pihak penerima, waktu transfer, serta hash ulang terhadap bukti pada saat diterima. Apabila hash hasil penghitungan ulang pada saat penerimaan tidak identik dengan hash pada entri sebelumnya, sistem akan menandai adanya potensi penyimpangan (*custody anomaly*) yang harus diklarifikasi sebelum bukti dapat dilanjutkan ke tahap berikutnya. Mekanisme ini secara langsung menjawab celah ketiga di atas, karena setiap entri tercatat secara real-time dan tidak dapat diubah secara retroaktif tanpa terdeteksi oleh seluruh node dalam jaringan, sejalan dengan karakteristik *append-only* yang ditekankan oleh Bonomi, Casini, dan Ciccotelli (2020) dalam rancangan B-CoC mereka.

Pada tahap keempat, hakim dan para pihak di persidangan dapat memverifikasi keaslian bukti digital secara mandiri dengan cara menghitung ulang nilai hash dari bukti yang disajikan dan mencocokkannya dengan nilai hash yang tersimpan pada entri terakhir di *distributed ledger*. Apabila kedua nilai hash identik, secara matematis dapat dipastikan bahwa bukti yang diajukan tidak mengalami perubahan sejak entri terakhir direkam. Mekanisme ini tidak menghilangkan peran keterangan ahli sama sekali, tetapi mengubah fungsinya dari satu-satunya dasar penilaian otentisitas menjadi alat bantu teknis untuk menjelaskan proses penghitungan hash kepada hakim yang tidak memiliki latar belakang teknis informatika.

Model rekonstruksi ini secara prinsip tidak bertentangan dengan asas *due process of law* maupun ketentuan alat bukti elektronik dalam Pasal 235 dan Pasal 241 KUHAP Baru, karena pencatatan blockchain pada dasarnya hanya memperkuat fungsi pembuktian administratif yang selama ini telah diwajibkan melalui berita acara, tanpa menggantikan syarat substantif keabsahan perolehan bukti. Pasal 241 KUHAP Baru secara eksplisit memperluas cakupan barang bukti hingga mencakup informasi dan dokumen elektronik yang memiliki keterkaitan langsung dengan dugaan tindak pidana, sehingga model rekonstruksi berbasis blockchain ini secara substansi memperkuat, bukan menggantikan, kerangka normatif yang telah dibangun KUHAP Baru. Dengan demikian, hasil rekonstruksi ini memiliki legitimasi hukum yang melekat pada kerangka KUHAP Baru itu sendiri, bukan sekadar usulan teknologis yang berdiri di luar sistem hukum acara pidana yang berlaku.

Rekonstruksi sistem pembuktian perkara pidana melalui implementasi teknologi blockchain bertujuan untuk menghasilkan suatu desain sistem pembuktian yang mampu menjamin integritas, transparansi, keamanan, dan ketertelusuran (*traceability*) barang bukti digital sejak pertama kali ditemukan pada tahap penyidikan hingga digunakan sebagai alat bukti dalam persidangan. Rekonstruksi ini didasarkan pada kebutuhan pembaruan mekanisme pembuktian dalam menghadapi perkembangan kejahatan berbasis teknologi informasi yang semakin kompleks. Sistem pembuktian konvensional yang masih mengandalkan pencatatan administrasi secara manual atau tersentralisasi memiliki berbagai kelemahan, seperti potensi perubahan data, hilangnya riwayat penguasaan barang bukti, serta kesulitan dalam membuktikan keaslian bukti digital ketika diajukan di persidangan. Oleh karena itu, teknologi blockchain dipilih sebagai instrumen yang mampu menyediakan mekanisme pencatatan digital yang bersifat permanen (*immutable*), terdistribusi (*distributed ledger*), dan dapat diverifikasi oleh seluruh pihak yang memiliki kewenangan tanpa memungkinkan adanya perubahan data secara sepihak.⁶

⁶ Stuart Haber & W. Scott Stornetta, "How to Time-Stamp a Digital Document," *Journal of Cryptology*, Vol. 3,

Tahap awal dalam rekonstruksi tersebut dilakukan melalui analisis terhadap kelemahan mekanisme Chain of Custody yang berlaku saat ini. Penelitian akan memetakan berbagai kerentanan hukum maupun teknis dalam proses penyimpanan, pemindahan, pemeriksaan laboratorium forensik, hingga penyajian barang bukti digital di persidangan. Kerentanan tersebut meliputi tidak adanya sistem pencatatan yang mampu menunjukkan riwayat perubahan penguasaan barang bukti secara real-time, terbatasnya mekanisme verifikasi terhadap kemungkinan modifikasi data digital, serta masih bergantungnya pembuktian pada dokumen administrasi yang dapat dipalsukan ataupun mengalami kehilangan. Pemetaan terhadap kelemahan tersebut menjadi dasar argumentasi ilmiah mengenai urgensi penerapan blockchain sebagai mekanisme pengamanan barang bukti digital yang lebih akuntabel dan mampu meningkatkan kepercayaan terhadap proses pembuktian dalam sistem peradilan pidana.⁷

Berdasarkan hasil identifikasi tersebut, penelitian ini merumuskan suatu protokol teknis implementasi blockchain pada tahap penyidikan. Setiap barang bukti digital yang diperoleh penyidik akan melalui proses akuisisi digital sesuai standar digital forensik, kemudian dibuatkan nilai hash menggunakan algoritma kriptografi sebagai identitas unik dari barang bukti tersebut. Selanjutnya, metadata yang memuat informasi mengenai waktu penyitaan (*timestamp*), identitas penyidik, lokasi penyitaan, jenis barang bukti, nilai hash, serta informasi pendukung lainnya akan dicatat ke dalam jaringan blockchain. Dengan mekanisme tersebut, data asli barang bukti tetap disimpan secara aman dalam media penyimpanan forensik, sedangkan blockchain berfungsi sebagai buku besar digital yang menyimpan catatan autentik mengenai seluruh aktivitas terhadap barang bukti. Setiap perubahan penguasaan, pemeriksaan laboratorium, maupun proses penyerahan kepada penuntut umum akan menghasilkan transaksi baru yang tercatat secara otomatis sehingga seluruh riwayat barang bukti dapat ditelusuri secara utuh sejak awal hingga akhir proses peradilan.⁸

Selain menghasilkan protokol penyidikan, penelitian ini juga merancang mekanisme Transfer of Custody berbasis blockchain. Setiap perpindahan penanggung jawab barang bukti, baik dari penyidik kepada laboratorium forensik, dari laboratorium kepada penuntut umum, maupun dari penuntut umum ke pengadilan, wajib dilakukan melalui proses autentikasi digital menggunakan tanda tangan elektronik dan pencatatan transaksi pada blockchain. Sistem ini menghasilkan jejak audit (*audit trail*) yang tidak dapat diubah (*immutable*) sehingga setiap pihak dapat mengetahui siapa yang menerima, menyerahkan, memeriksa, maupun menyimpan barang bukti beserta waktu pelaksanaannya secara akurat. Dengan demikian, kemungkinan manipulasi terhadap rantai penguasaan barang bukti dapat diminimalkan karena setiap perubahan akan meninggalkan jejak digital yang dapat diverifikasi sewaktu-waktu oleh aparat penegak hukum maupun hakim.⁹

Pada tahap persidangan, model rekonstruksi ini menghasilkan standar verifikasi autentikasi barang bukti digital yang lebih sederhana namun memiliki tingkat keandalan tinggi. Hakim, penuntut umum, penasihat hukum, maupun ahli digital forensik cukup melakukan perhitungan ulang terhadap nilai hash dari barang bukti yang diajukan di persidangan dan membandingkannya dengan nilai hash yang telah tersimpan di blockchain

No. 2 (1991), hlm. 99–111.

⁷ National Institute of Standards and Technology (NIST), *Blockchain Technology Overview* (NISTIR 8202) (Gaithersburg: U.S. Department of Commerce, 2018), hlm. 1–15.

⁸ National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response* (Special Publication 800-86), U.S. Department of Commerce, 2006, hlm. 3–15.

⁹ Marco Iansiti & Karim R. Lakhani, "The Truth About Blockchain," *Harvard Business Review*, Vol. 95, No. 1 (2017), hlm. 118–127.

sejak proses penyitaan. Apabila kedua nilai tersebut identik, maka dapat dipastikan bahwa barang bukti tidak mengalami perubahan sedikit pun selama proses penanganan. Sebaliknya, apabila ditemukan perbedaan nilai hash, sistem secara langsung menunjukkan bahwa telah terjadi perubahan terhadap data sehingga autentisitas barang bukti patut dipertanyakan. Mekanisme ini memberikan jaminan kepastian hukum yang lebih kuat terhadap pembuktian elektronik sekaligus mengurangi ketergantungan pembuktian pada keterangan saksi ahli semata. Seluruh model rekonstruksi tersebut tetap disusun dengan mengacu pada asas *due process of law*, prinsip keaslian alat bukti elektronik, serta ketentuan mengenai pembuktian dalam KUHAP berdasarkan Undang-Undang Nomor 20 Tahun 2025, sehingga implementasinya tidak hanya layak secara teknis, tetapi juga memiliki legitimasi yuridis dalam sistem peradilan pidana Indonesia.¹⁰

C. Implikasi terhadap Exclusionary Rule dan Kepastian Hukum

Identifikasi terhadap mekanisme hash cryptography, timestamp, dan distributed ledger pada subbagian sebelumnya menghasilkan kerangka prosedur hipotetik (*hypothetical SOP*) mengenai tata cara pengikatan bukti digital ke dalam rantai blok yang sesuai dengan amanat Pasal 235 mengenai syarat autentikasi.

Kodifikasi *exclusionary rule* dalam Pasal 235 KUHAP Baru tidak berdiri sendiri sebagai norma domestik, melainkan merupakan pelaksanaan atas dua kewajiban hukum internasional yang telah mengikat Indonesia.

Pertama, Pasal 14 ayat (3) *International Covenant on Civil and Political Rights* (ICCPR) menjamin hak setiap orang yang didakwa dalam perkara pidana atas peradilan yang adil (*fair trial*), termasuk hak untuk tidak dipaksa memberikan kesaksian yang memberatkan diri sendiri atau mengakui kesalahan sebagaimana diatur pada huruf (g)¹¹. Komite HAM PBB melalui General Comment No. 32 menegaskan jaminan tersebut berkaitan erat dengan larangan penyiksaan dalam Pasal 7 ICCPR, sehingga pernyataan atau bukti hasil penyiksaan wajib dikesampingkan, kecuali sebagai bukti bahwa penyiksaan itu terjadi. *Fair trial* dalam konteks ini menuntut agar kebenaran materiil tidak dibangun di atas fondasi yang tercemar pelanggaran HAM.

Kedua, Pasal 15 *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (CAT/Konvensi Anti Penyiksaan) secara tegas mewajibkan setiap negara pihak untuk memastikan bahwa setiap pernyataan yang terbukti diperoleh melalui penyiksaan tidak dapat digunakan sebagai bukti dalam persidangan manapun, kecuali terhadap pelaku penyiksaan itu sendiri sebagai bukti bahwa pernyataan tersebut telah dibuat¹². Ketentuan ini bersifat *non-derogable* dan tidak dapat disimpangi bahkan dalam keadaan darurat. Indonesia terikat pada kedua instrumen tersebut sebagai negara pihak, masing-masing melalui Undang-Undang Nomor 12 Tahun 2005 dan Undang-Undang Nomor 5 Tahun 1998¹³, sehingga Pasal 235 ayat (1) huruf h dan ayat (5) KUHAP Baru pada hakikatnya merupakan transformasi domestik atas kewajiban internasional tersebut.

Titik temu Pasal 235 KUHAP Baru dengan ICCPR dan CAT relevan bagi model rekonstruksi *chain of custody* berbasis blockchain pada Sub-bab B. Hash cryptography hanya menjamin data tidak berubah sejak dicatat; ia tidak dapat menjamin bahwa interogasi,

¹⁰ Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana; National Institute of Standards and Technology (NIST), *Blockchain Technology Overview* (NISTIR 8202), 2018.

¹¹ *International Covenant on Civil and Political Rights*, Pasal 14 ayat (3) huruf g, 16 Desember 1966, 999 UNTS 171; UN Human Rights Committee, General Comment No. 32, CCPR/C/GC/32, 23 Agustus 2007, para. 6 dan 41.

¹² *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, Pasal 15, 10 Desember 1984, 1465 UNTS 85.

¹³ Indonesia meratifikasi ICCPR melalui Undang-Undang Nomor 12 Tahun 2005 dan Konvensi Menentang Penyiksaan melalui Undang-Undang Nomor 5 Tahun 1998.

penyitaan gawai, atau ekstraksi data yang mendahului pencatatan bebas dari paksaan atau perlakuan merendahkan martabat manusia. Kepatuhan teknis atas autentikasi kriptografis karenanya tidak pernah menggantikan penilaian yudisial independen atas ada tidaknya pelanggaran Pasal 7 ICCPR atau Pasal 15 CAT pada tahap perolehan bukti.

Penguatan integritas bukti melalui arsitektur blockchain tidak dapat dilepaskan dari konsekuensinya terhadap hak atas privasi. Dua dimensi ketegangan perlu diperhatikan.

Pertama, perlindungan data pribadi menuntut agar informasi yang melekat pada tersangka, saksi, atau pihak ketiga tidak terkait langsung dengan tindak pidana tidak diproses melebihi keperluan penegakan hukum yang sah. Sifat distributed ledger yang direplikasi ke banyak simpul berpotensi memperluas eksposur data pribadi apabila desain sistem tidak secara ketat membatasi pencatatan pada metadata dan nilai hash.

Kedua, pembatasan tujuan pengolahan data (purpose limitation) menjadi persoalan tersendiri berhadapan dengan sifat immutable blockchain. Prinsip ini mensyaratkan data pribadi hanya diproses untuk tujuan spesifik penegakan hukum dan wajib dihapus atau dianonimkan setelah perkara berakhir, sementara karakteristik ledger yang permanen dan append-only berpotensi berbenturan langsung dengan hak tersebut karena data tetap tersimpan meski kepentingan penegakan hukum atasnya telah hilang.

Pasal 235 KUHAP Baru telah mengodifikasi exclusionary rule secara eksplisit, penelusuran terhadap norma yang ada menunjukkan tiga kesenjangan yang berdampak pada efektivitas perlindungan HAM.

Pertama, KUHAP Baru belum mengatur secara eksplisit doktrin fruit of the poisonous tree, yaitu bahwa bukti turunan dari bukti primer yang cacat prosedural turut kehilangan keabsahannya. Pasal 235 ayat (5) dapat ditafsirkan ekstensif mencakup logika tersebut, namun ketiadaan rumusan tegas menyisakan ruang penafsiran berbeda antarahakim dan berpotensi menimbulkan disparitas putusan, khususnya dalam perkara penyidikan digital berlapis, misalnya ketika akses awal terhadap suatu akun elektronik diperoleh melawan hukum namun datanya digunakan untuk memperoleh izin penggeledahan lanjutan.

kedua, belum tersedia mekanisme peninjauan pra-persidangan (pre-trial evidentiary hearing) untuk menguji keabsahan perolehan bukti digital sebelum pemeriksaan pokok perkara. Akibatnya pengujian baru dilakukan di persidangan pokok, sehingga apabila bukti akhirnya dinyatakan tidak sah, sumber daya peradilan menjadi tidak efisien dan masa penahanan terdakwa berpotensi memanjang, bersinggungan dengan hak atas peradilan tanpa penundaan tidak beralasan pada Pasal 14 ayat (3) huruf c ICCPR.

Hasil analisis menunjukkan bahwa blockchain bukanlah "tiket bebas" dari pelanggaran prosedur penggeledahan atau penyitaan. Doktrin exclusionary rule, yang kini dikodifikasi secara eksplisit melalui Pasal 235 ayat (1) huruf h dan ayat (5) KUHAP Baru, bekerja pada tataran keabsahan perolehan (materiil), sedangkan integritas kriptografis blockchain bekerja pada tataran keaslian data pasca-perolehan (formil). Kedua tataran ini bersifat independen, sehingga sekuat apa pun rantai hash yang dibangun, jika bukti digital tersebut pada awalnya diperoleh melalui cara yang melanggar hukum, misalnya melalui penyadapan tanpa izin pengadilan sebagaimana disyaratkan dalam kerangka upaya paksa KUHAP Baru, maka bukti tersebut tetap harus dikesampingkan demi hukum. Penegasan ini sejalan dengan ketentuan Pasal 235 ayat (4) yang memberikan kewenangan kepada hakim untuk menilai keabsahan perolehan alat bukti secara terpisah dari penilaian autentikasinya, serta konsisten dengan logika doktrin fruit of the poisonous tree yang tercermin dalam Pasal 235 ayat (5), yaitu bahwa alat bukti turunan dari bukti yang diperoleh secara melawan hukum turut kehilangan keabsahannya. Dengan demikian, titik batas (boundary) yang dapat dirumuskan adalah bahwa blockchain hanya relevan pada saat hakim telah memastikan keabsahan perolehan bukti secara materiil; teknologi ini tidak dapat dan tidak boleh digunakan untuk "mencuci" cacat prosedural pada tahap perolehan.

Pada aspek kepastian hukum, penerapan blockchain memberikan sejumlah manfaat strategis sekaligus menyisakan risiko yuridis yang perlu diantisipasi, sebagaimana dipetakan pada Tabel 2.

Tabel 2 Pemetaan Manfaat dan Risiko Yuridis Penerapan Blockchain pada Sistem Pembuktian Pidana

Aspek	Manfaat (Sisi Positif)	Risiko (Sisi Kritis)
Autentisitas	Validasi matematis-kriptografis menghilangkan keraguan subjektif hakim atas keaslian bukti	Belum ada Peraturan Pemerintah/Peraturan MA yang mengatur standar teknis blockchain forensik
Transparansi	Jejak audit (audit trail) transparan dan dapat ditelusuri oleh seluruh pihak berwenang	Keterbatasan kemampuan hakim menilai bukti teknis tanpa bantuan ahli forensik digital
Resistensi manipulasi	Mempersempit ruang fabrikasi, penggantian, atau kontaminasi bukti oleh oknum	Potensi disparitas putusan akibat perbedaan pemahaman teknologi antarahakim/antarpengadilan
Efisiensi pembuktian	Mengurangi ketergantungan mutlak pada keterangan ahli untuk membuktikan keaslian	Risiko over-reliance pada validitas teknis tanpa menilai keabsahan materiil perolehan

Tabel 2 menggambarkan bahwa manfaat blockchain bersifat signifikan pada dimensi formal pembuktian, tetapi risiko yuridisnya justru muncul dari kekosongan kerangka regulasi pelaksana. Hingga saat penelitian ini dilakukan, belum tersedia Peraturan Pemerintah maupun Peraturan Mahkamah Agung yang secara eksplisit mengatur standar teknis penerapan distributed ledger pada penanganan bukti digital, sehingga implementasinya pada praktik peradilan pidana berpotensi berjalan tidak seragam antarwilayah hukum. Risiko lain yang relevan adalah keterbatasan kapasitas hakim dalam menilai bukti teknis tanpa bantuan ahli forensik digital, yang apabila tidak diantisipasi dapat menimbulkan disparitas putusan, sebagaimana juga diperingatkan dalam temuan Onyeashie, Leimich, McKeown, dan Russell (2024) bahwa adopsi teknologi forensik baru kerap mendahului kesiapan kapasitas institusional penegak hukum maupun peradilan.

Pengujian terhadap fleksibilitas Pasal 235 ayat (3), (4), dan (5) menunjukkan bahwa norma tersebut, meskipun dirumuskan secara netral teknologi (technology neutral), cukup terbuka untuk mengakomodasi pembuktian berbasis blockchain melalui penafsiran ekstensif terhadap frasa "autentik" dan "diperoleh secara tidak melawan hukum". Frasa "autentik" dalam konteks bukti elektronik dapat ditafsirkan mencakup kesesuaian nilai hash antara bukti yang disajikan dengan entri yang tersimpan pada ledger, sebagai pelengkap pembuktian autentikasi konvensional melalui keterangan ahli. Sementara itu, frasa "diperoleh secara tidak melawan hukum" tetap harus dimaknai merujuk pada kepatuhan terhadap syarat formil Pasal 113, 116, 119, dan 124 sebagaimana telah diuraikan pada subbagian sebelumnya, terlepas dari kecanggihan teknologi yang digunakan untuk mengamankan bukti pasca-perolehan. Tafsir hukum baru ini penting untuk mencegah miskonsepsi di tingkat praktik bahwa "bukti yang tercatat di blockchain otomatis sah", sebuah miskonsepsi yang apabila dibiarkan justru akan melemahkan, bukan memperkuat, prinsip kepastian hukum yang hendak dicapai.

Temuan Fahririn et al. (2026) tentang kelemahan sistem keamanan data dalam perlindungan whistleblower di Indonesia memperkuat argumen bahwa blockchain tidak dapat berdiri sendiri sebagai solusi teknis. Dalam kasus pelapor korupsi yang identitasnya terpapar di dark web, sekuat apa pun enkripsi blockchain, jika sumber data awal tidak dilindungi secara memadai, maka celah keamanan tetap eksis. Dengan demikian, sinergi antara regulasi perlindungan data dan teknologi blockchain menjadi prasyarat mutlak bagi terwujudnya sistem pembuktian pidana yang adil dan aman di era digital.

Sebagai sintesis akhir, penelitian ini merumuskan usulan konstruksi hukum baru yang memadukan tiga unsur, yaitu chain of custody berbasis blockchain sebagai aspek teknis, exclusionary rule sebagai filter yudisial pada aspek hak asasi manusia, dan kepastian hukum sebagai payung akhir aspek keadilan prosedural. Ketiga unsur tersebut dapat dirumuskan dalam bentuk rancangan konsep omnibus prosedural yang memuat: (a) kewajiban pencatatan hash dan metadata izin pengadilan sebagai entri pertama ledger; (b) kewajiban pencatatan setiap transfer custody secara real-time; (c) hak hakim dan para pihak untuk melakukan verifikasi hash secara mandiri; dan (d) penegasan bahwa kecocokan hash tidak menggantikan, melainkan melengkapi, penilaian keabsahan perolehan bukti oleh hakim. Konstruksi ini dapat direkomendasikan kepada Mahkamah Agung dalam bentuk Surat Edaran atau Peraturan Mahkamah Agung, maupun kepada Dewan Perwakilan Rakyat dan Pemerintah dalam bentuk peraturan pelaksana di bawah UU No. 20 Tahun 2025, sehingga inovasi teknologi yang ditawarkan tidak berdiri sebagai usulan teknologis semata, tetapi terintegrasi secara koheren ke dalam kerangka hukum acara pidana yang berlaku.

KESIMPULAN

Penelitian ini menyimpulkan bahwa mekanisme chain of custody bukti digital berbasis blockchain dapat diimplementasikan untuk memenuhi standar penggeledahan dan penyitaan dalam KUHAP Baru, dengan syarat entri awal (genesis entry) pada distributed ledger secara eksplisit mengaitkan hash dan metadata bukti dengan nomor izin atau penetapan persetujuan ketua pengadilan negeri sebagaimana diatur dalam Pasal 113, 116, 119, dan 124. Empat dari lima parameter kepatuhan yang diuji terpenuhi secara teknis oleh mekanisme blockchain, sementara keabsahan perolehan awal bukti tetap merupakan penilaian yuridis yang tidak dapat digantikan oleh teknologi apa pun.

Rekonstruksi sistem pembuktian perkara pidana tercapai melalui model empat tahap, yaitu penemuan dan penyitaan bukti, penghitungan hash serta pengunggahan metadata, pencatatan setiap transfer custody sebagai entri immutable, dan verifikasi mandiri oleh hakim pada tahap persidangan, yang dijalankan di atas arsitektur hybrid on-chain/off-chain. Model ini menjamin integritas, transparansi, dan ketelusuran barang bukti digital sepanjang siklus penyidikan hingga persidangan tanpa perlu menyimpan konten substantif bukti pada ledger yang bersifat permanen, sehingga sekaligus melindungi hak privasi pihak yang berperkara.

Implikasinya terhadap exclusionary rule, penelitian ini menyimpulkan bahwa verifikasi kriptografis berbasis blockchain bekerja pada tataran keaslian data pasca-perolehan dan tidak dapat menggantikan maupun memulihkan keabsahan perolehan bukti secara materiil. Sekuat apa pun rantai hash yang dibangun, bukti digital yang diperoleh secara melawan hukum tetap harus dikesampingkan, sejalan dengan logika fruit of the poisonous tree yang tercermin dalam Pasal 235 ayat (5) KUHAP Baru. Dengan demikian, kepastian hukum dalam sistem pembuktian pidana hanya dapat dicapai apabila kepatuhan teknis terhadap Pasal 235 diiringi kepatuhan prosedural sejak tahap penggeledahan dan penyitaan, sehingga ketiga tujuan penelitian ini, yakni terciptanya kepastian hukum, minimalisasi fabricated evidence, dan terjaminnya due process of law, dapat tercapai secara kumulatif dan tidak dapat dipenuhi oleh teknologi secara berdiri sendiri.

Sebagai tindak lanjut, penelitian ini merekomendasikan agar Mahkamah Agung atau Pemerintah menerbitkan peraturan pelaksana yang secara eksplisit mewajibkan keterkaitan antara entri distributed ledger dengan otorisasi penggeledahan atau penyitaan dari pengadilan. Penelitian lanjutan yang bersifat empiris juga diperlukan untuk menguji kesiapan infrastruktur teknologi dan kapasitas sumber daya manusia aparat penegak hukum, serta melakukan kajian komparatif terhadap yurisdiksi lain yang telah menerapkan mekanisme serupa, guna memperkuat validitas model rekonstruksi chain of custody berbasis blockchain yang dirumuskan dalam penelitian ini.

DAFTAR PUSTAKA

- Bonomi, S., Casini, M., & Ciccotelli, C. (2020). B-CoC: A blockchain-based chain of custody for evidences management in digital forensics. *Proceedings of the 2nd International Conference on Blockchain Technology*, 1–8. <https://doi.org/10.4230/OASICS.Tokenomics.2019.12>
- Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. (1984, 10 Desember). 1465 UNTS 85. <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-against-torture-and-other-cruel-inhuman-or-degrading>
- Dylan Yaga (NIST), Peter Mell (NIST), Nik Roby (G2), Karen Scarfone (Scarfone Cybersecurity). National Institute of Standards and Technology. (2018). *Blockchain Technology Overview* (NISTIR 8202). Gaithersburg: U.S. Department of Commerce. <https://csrc.nist.gov/pubs/ir/8202/final>
- Fahrir, F., MY, A. S., & Nut, N. (2025). Digital Transformation of Whistleblower Legal Protection in Eradicating Corruption in Indonesia. *Journal Evidence Of Law*, 4(3), 1211–1220. <https://doi.org/10.59066/jel.v4i3.1742>
- Haber, S., Stornetta, W.S. How to time-stamp a digital document. *J. Cryptology* 3, 99–111 (1991). <https://doi.org/10.1007/BF00196791>
- Hamzah, A. (2019). *Hukum Acara Pidana Indonesia*. Jakarta: Sinar Grafika.
- Hukumonline. (2026). Jenis alat bukti sah menurut KUHAP baru. Klinik Hukumonline. <https://www.hukumonline.com/klinik/a/jenis-alat-bukti-sah-menurut-kuhap-baru-lt657ae25924ac9/>
- Iansiti, Marco., & Lakhani, Karim R. (2017). The Truth About Blockchain. *Harvard Business Review*, 95(1), 118–127. <https://hbr.org/2017/01/the-truth-about-blockchain>
- Indonesia. (1998). Undang-Undang Nomor 5 Tahun 1998 tentang Pengesahan Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.
- Indonesia. (2005). Undang-Undang Nomor 12 Tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights. <https://peraturan.bpk.go.id/Details/40261/uu-no-12-tahun-2005>
- Indonesia. (2025). Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.
- Indonesia. (2025). Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Pidana.
- International Covenant on Civil and Political Rights. (1966, 16 Desember). 999 UNTS 171. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- Kent.,K, Chevalier,,S.Grance, Hung Dang. National Institute of Standards and Technology. (2006). *Guide to Integrating Forensic Techniques into Incident Response* (Special Publication 800-86). Gaithersburg: U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/86/final>
- Lakada, D. D. J., Antouw, D. T., & Bawole, G. Y. (2024). Perkembangan pengaturan alat bukti elektronik dalam hukum acara pidana (kajian hukum tentang cyber crime). *Lex Crimen*, 12(4), 1–15. <https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/591>
- Lone, A. H., & Mir, R. N. (2017). Forensic-chain: Ethereum blockchain based digital forensics chain of custody. *Scientific and Practical Cyber Security Journal*, 1(2), 21–27. <https://journal.scsa.ge/papers/forensic-chain-ethereum-blockchain-based-digital-forensics-chain-of-custody/>

- Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, 28, 44–55. <https://doi.org/10.1016/j.diin.2019.01.002>
- Mahkamah Agung RI. (2026). KUHAP baru: Adaptasi pembuktian di era digital. *MariNews*. <https://marinews.mahkamahagung.go.id/>
- Megawati, Leny., Wiharma, Cecep., & Hasanudin, Asep. (2023). Peran Teknologi Blockchain dalam Meningkatkan Keamanan dan Kepastian Hukum dalam Transaksi Kontrak di Indonesia. *Jurnal Hukum Mimbar Justitia*, 9(2), 412. <https://doi.org/10.35194/jhmj.v9i2.3856>
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>
- Onyeashie, B. I., Leimich, P., McKeown, S., & Russell, G. (2024). A Bibliometric Analysis and Systematic Review of a Blockchain-Based Chain of Custody for Digital Evidence. *Big Data Technologies and Applications*. BDTA 2023. Springer. https://doi.org/10.1007/978-3-031-52265-9_8
- Patil, H., Kohli, R.K., Puri, S. et al. Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework. *Egypt J Forensic Sci* 14, 12 (2024). <https://doi.org/10.1186/s41935-023-00383-w>
- Ramadhan, Kurnia. (2023, 5 Agustus). Chain Of Custody berbasis Blockchain dalam Penanganan Bukti Digital. *Hukumonline.com*. <https://www.hukumonline.com/berita/a/chain-of-custody-berbasis-blockchain-dalam-penanganan-bukti-digital-lt64ce49bc3bf67/>
- Ramiyanto. (2017). Bukti elektronik sebagai alat bukti yang sah dalam hukum acara pidana. *Jurnal Hukum dan Peradilan*, 6(3), 473–485. DOI : 10.25216/JHP.6.3.2017.463-486
- Surya, Arif Putra., & Prayudi, Yudi. (2021). Implementasi Multi Smart Contract pada Bukti Digital dan Chain of Custody dalam Meningkatkan Keamanan dan Integritas Bukti Digital. *JUSTINDO*, 6(2), 100. <https://doi.org/10.32528/justindo.v6i2.3945>
- United Nations Human Rights Committee. (2007). General Comment No. 32: Right to Equality Before Courts and Tribunals and to a Fair Trial (CCPR/C/GC/32). New York: United Nations. <https://digitallibrary.un.org/record/606075?v=pdf>