



KOMTELKA: Jurnal Komputer Telekomunikasi
dan Elektronika, Volume 01 Nomor 1 Tahun
2026

Tersedia online di

<https://jurnal.rajawalicemerlangabadi.com/index.php/jpek>



Tinjauan Yuridis Kejahatan Siber Aset Kripto: Akses Ilegal dan Pencurian dalam UU ITE dan KUHP

Nasywa Karini Qonita¹, Allyssa Nadilla Putri², Elsha Intan Parwanti³, Yuliarman Saragih⁴

^{1,2,3,4}Universitas Singaperbangsa Karawang

email: ¹2510631010166@student.unsika.ac.id, ²2510631010086@student.unsika.ac.id,

³2510631010110@student.unsika.ac.id, ⁴yuliarman@yahoo.com

Kata kunci:

Peninggalan Kripto
Akses Ilegal
UU ITE
Blockchain
Kejahatan Siber

ABSTRAK

Perkembangan peninggalan kripto menghasilkan celah hukum di Indonesia. Riset normatif yuridis ini mengkaji status hukum kripto selaku "benda" (Pasal 362 KUHP) ataupun "data" (UU ITE), penegakan hukum terpaut akses ilegal dalam peretasan dompet awan, dan tantangan dalam pembuktian sebab watak anonimitas dari blockchain. Penemuan riset menampilkan kalau pengenaan dakwaan kumulatif- alternatif di dasar Pasal 362 KUHP serta Pasal 30 UU ITE membagikan pemecahan yang instan. Tantangan utama yang dialami meliputi batas dalam forensik digital, yurisdiksi lintas negeri, dan autentikasi fakta elektronik. Peraturan spesial serta kenaikan kapasitas penyidikan sangat diperlukan.

Keywords:

Crypto Aset
Illegal Access
ITE Act
Blockchain
Cybercrime

ABSTRACT

The emergence of cryptocurrency leads to sah gaps in Indonesia. This study employs normative sah analysis to assess the sah classification of cryptocurrency as "object" (Article 362 of the Criminal Code) or "data" (ITE Act), the enforcement of laws regarding illegal access to cloud wallet hacking, and the difficulties in proving cases due to the anonymity inherent in blockchain technology. The results indicate that alternative- cumulative charges under Article 362 of the Criminal Code and Article 30 of the ITE Act present a practical approach to these issues. Major obstacles include limitations in digital forensic techniques, jurisdictional issues across borders, and the authentication of electronic evidence. There is an urgent need for specialized regulation and an increase in investigative capabilities.

PENDAHULUAN

Pasar cryptocurrency di Indonesia berkembang dengan kilat; volume transaksi diperkirakan hendak lebih dari Rp 650 triliun pada tahun 2024, bersumber pada data dari Bappebti [1]. Bersamaan dengan pertumbuhan ini, kejahatan siber yang menargetkan duit kripto – seperti peretasan dompet digital, penipuan phishing, serta

pencurian kunci pribadi—semakin bertambah, baik dari segi jumlah peristiwa ataupun tingkatan kesulitannya. Peraturan yang terdapat dikala ini—yaitu Kitab Undang- Undang Hukum Pidana (KUHP), Undang- Undang Transaksi Informasi serta Elektronik (UU No 11 Tahun 2008 serta perubahannya), dan Undang- Undang Perlindungan Data Orang (UU No 27 Tahun 2022) – belum menarangkan dengan jelas menimpa kejahatan yang berkaitan dengan peninggalan digital [2].

Terdapat ketidakpastian hukum di 2 aspek. Awal, apakah kerugian yang disebabkan oleh peretasan terhadap peninggalan kripto dapat di tuntutan bersumber pada Pasal 362 KUHP yang mengendalikan tentang pencurian, ataupun Pasal 30 UU ITE yang mengendalikan tentang akses tanpa izin. Kedua, gimana metode meyakinkan kejahatan ini, mengingat watak pseudo- anonim dari blockchain. Pedoman Jaksa Agung No 7 Tahun 2023 sudah membagikan panduan tentang metode penyitaan mata duit kripto selaku benda yang berwujud, tetapi masih terdapat permasalahan terpaut tanggung jawab pidana yang belum dibahas secara merata [3].

Studi ini bertujuan buat mangulas 3 perihal: (1) apakah peninggalan kripto dapat dikira selaku “benda” bagi Pasal 362 Kitab Undang- Undang Hukum Pidana ataupun selaku “data” bagi Undang- Undang ITE; (2) gimana pelaksanaan Pasal 30 Undang- Undang ITE dalam permasalahan peretasan dompet cloud; serta (3) tantangan apa yang dialami dalam meyakinkan kasus- kasus ini mengingat watak anonim yang terdapat pada blockchain. Tujuan dari riset ini merupakan buat menganalisis kondisi hukum dari peninggalan kripto, mengecek penerapan akses yang tidak legal, serta menyusun anjuran buat regulasi.

METODE PENELITIAN

Studi ini memakai tata cara hukum normatif dengan 3 pendekatan yang silih terpaut: (1) pendekatan yuridis, yang menganalisis Kitab Undang- Undang Hukum Pidana (KUHP), Undang- Undang ITE, Undang- Undang Proteksi Informasi Individu (UU PDP), serta peraturan dari Bappebti/ OJK; (2) pendekatan konseptual, yang menekuni doktrin “benda”, “data”, serta “akses ilegal”; dan (3) pendekatan komparatif, yang memandang pelaksanaan regulasi di Jerman serta Singapore. Bahan- bahan hukum dikumpulkan dengan metode mencari data dari Google Scholar serta

Garuda Kemdikbud buat tahun 2020 hingga 2025. Sehabis itu, informasi tersebut dianalisis dengan tata cara kualitatif memakai interpretasi gramatikal, sistematis, serta teleologis.

Tabel 1 di dasar ini menampilkan perbandingan norma antara 2 peraturan utama yang silih berkaitan, yang jadi fokus analisis buat riset ini.

Tabel 1. Perbandingan Regulasi Kejahatan Siber terhadap Aset Kripto

Aspek	KUHP Pasal 362	UU ITE Pasal 30 Ayat (3)
Objek	"Benda" bernilai murah (tercantum peninggalan intangible bersumber pada ekspansi doktrin)	"Sistem elektronik" serta data elektronik, tercantum kunci privat kripto
Perbuatan	Mengambil tanpa hak dengan iktikad memiliki	Mengakses/menerobos/m enjebol sistem pengamanan tanpa hak
Sanksi	Sanksi Penjara maks. 5 tahun	Penjara maks. 8 tahun serta/ ataupun denda Rp 800 juta
Kendala	Unsur "mengambil" mensyaratkan perpindahan raga; kripto bertabiat intangible	Belum menyebut kripto secara eksplisit; tergantung pada interpretasi hakim

PEMBAHASAN

1) Kedudukan Hukum Aset Kripto: "Benda" (KUHP) ataupun "Data" (UU ITE)?

Pasal 362 KUHP melaporkan kalau objek pencurian wajib berbentuk "benda." Bersumber pada pertumbuhan doktrin hukum internasional, tercantum permasalahan Electriciteitsarrest di Belanda pada tahun 1921, "benda" pula mencakup hal-hal yang tidak berwujud namun mempunyai nilai ekonomi. Aset kripto mempunyai identitas berikut: mempunyai nilai ekonomi yang dapat diukur, bisa dikendalikan secara eksklusif dengan kunci privat, serta dapat dipindahkan. Tetapi, tantangan utama terdapat pada aspek "mengambil" yang umumnya memerlukan perpindahan fisik, sebaliknya pencurian kripto cuma memindahkan kontrol yang berkaitan dengan kriptografi.

Di sisi lain, Pasal 30 ayat (3) jo. Pasal 32 UU ITE membagikan proteksi terhadap "sistem elektronik" serta "data elektronik" yang secara langsung mencakup kunci privat kripto. Kategorisasi ganda ini membolehkan terdapatnya dakwaan kumulatif alternatif bersumber pada Pasal 362 KUHP jo. Pasal 30 UU ITE merupakan penyelesaian instan yang dianjurkan disaat *lex specialis* belum ada. UU PDP Nomor. 27 Tahun 2022 pula menguatkan proteksi sebab informasi autentikasi kripto diduga sebagai "informasi individu" yang dilindungi oleh Pasal 67 [4].

2) Pelaksanaan Akses Ilegal terhadap Peretasan Cloud Wallet Kripto

Metode peretasan wallet cloud tercantum phishing, pengisian kredensial, serbuan man-in-the-middle, serta pergantian SIM. Pasal 30 ayat (3) UU ITE menetapkan 4 ketentuan: (a) dilakukan dengan terencana; (b) tanpa izin; (c) mengakses sistem elektronik; serta (d) mengganggu ataupun menembus sistem keamanan. Seluruh 4 ketentuan wajib terdapat bersama-sama dalam tiap permasalahan peretasan wallet. Ancaman hukuman dalam Pasal 46 ayat (3) UU ITE yakni penjara sangat lama 8 tahun serta/ maupun denda sebesar Rp 800 juta [5]. Hukuman ini lebih berat dibanding dengan Pasal 362 KUHP yang cuma 5 tahun. Oleh sebab itu, hukuman ini lebih cocok dengan kerugian yang ditimbulkan. Dengan diterapkannya KUHP Baru (UU Nomor. 1 Tahun 2023) secara lengkap pada tahun 2026, ketentuan ini bakal berpindah ke Pasal 332 dengan struktur yang sama [6].

3) Gangguan Pembuktian dalam Konteks Anonimitas Blockchain

Blockchain mempunyai sifat pseudoanonim: tiap transaksi dicatat secara permanen serta dapat dilihat oleh publik, namun alamat wallet cuma berbentuk campuran angka serta huruf tanpa identitas sesungguhnya. Gangguan dalam pembuktian terdiri dari 3 aspek: (1) teknis, ialah minimnya perlengkapan forensik blockchain di Bareskrim Polri serta sedikitnya personel yang terlatih guna analisis on-chain; (2) yurisdiksi, di mana watak internasional dari kejahatan kripto membutuhkan Perjanjian Pertolongan Hukum Timbal Balik (MLAT) yang masih kurang mencukupi; serta (3) prosedural, ialah fakta digital perlu diautentikasi cocok dengan standar Pasal 5 UU ITE, tapi verifikasi integritasnya masih jadi perdebatan di pengadilan [7].

Titik utama guna mengidentifikasi pelaku merupakan bursa terpusat yang wajib mempraktikkan KYC/ AML [8]. Kerja sama dengan bursa dalam negara yang terdaftar di OJK serta bursa internasional sangat berarti buat menguak permasalahan ini. Dibutuhkan: (1) pembuatan ketentuan eksklusif mengenai kejahatan aset digital; (2) peningkatan keterampilan forensik Bareskrim; (3) Peraturan Pemerintah yang memenuhi Pedoman Jaksa Agung Nomor. 7 Tahun 2023; serta (4) bergabung dengan Kesepakatan Budapest tentang Kejahatan Siber [9].

KESIMPULAN

Studi ini merumuskan 3 hal. pertama, aset kripto bisa dikenakan tuduhan berlandaskan Pasal 362 KUHP dan Pasal 30 UU ITE karena dikira selaku "benda" dalam arti yang luas dan pula sebagai objek akses ilegal. Namun, masih diperlukan syarat eksklusif yang lebih lengkap guna membetulkan kepastian hukum. Kedua, Pasal 30 ayat (3) UU ITE bisa menanggulangi peretasan wallet cloud secara hukum karna segala aspek kejahatan sudah terpenuhi, dengan ancaman hukuman yang lebih sesuai dibandingkan dengan KUHP. Ketiga, kasus dalam pembuktian bukan karena tidak ada jejak digital dari blockchain yang menaruh catatan transaksi secara permanen, tetapi karna ada batas teknis dalam forensik, yurisdiksi yang lintas negara, dan standar guna mengautentikasi kenyataan. Saran kebijakan: lekas buat syarat eksklusif mengenai kejahatan siber yang berkaitan dengan peninggalan digital, tingkatkan keahlian teknis penyidik, dan dorong buat bergabung dengan Konvensi Budapest biar kerja sama internasional terus jadi kuat.

DAFTAR PUSTAKA

- [1]. B. P. P. B. Komoditi, "Peraturan Bappebti Nomor 8 Tahun 2021 tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto di Bursa Berjangka," 2021, Bappebti. [Online]. Available: https://bappebti.go.id/pbk/sk_kep_kepala_bappebti/detail/8952
- [2]. P. R. Indonesia, "Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik," 2024, BPK RI. [Online]. Available: <https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024>
- [3]. K. A. R. Indonesia, "Pedoman Jaksa Agung Nomor 7 Tahun 2023 tentang Penanganan Aset Kripto sebagai Barang Bukti dalam Perkara Pidana," 2023, Kejaksaan Agung RI. [Online]. Available: <https://jdih.kejaksaan.go.id>

-
- [4]. P. R. Indonesia, "Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," 2022, BPK RI. [Online]. Available: <https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022>
 - [5]. P. R. Indonesia, "Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana," 2023, BPK RI. [Online]. Available: <https://peraturan.bpk.go.id/Home/Details/234935/uu-no-1-tahun-2023>
 - [6]. Murizqy and Dirkareshza, "Peninjauan Aspek Keamanan dan Perlindungan Hukum terhadap Investor Cryptocurrency," J. Ius Const., vol. 7, no. 2, pp. 277–292, 2022, doi: <https://doi.org/10.26623/jic.v7i2.4067>.
 - [7]. M. D. Pane and E. Siahaan, "TINJAUAN YURIDIS MENGENAI TANGGUNG JAWAB PELAKU TINDAK PIDANA PENCURIAN: ANALISIS BERDASARKAN PASAL 362 KITAB UNDANG- UNDANG HUKUM PIDANA (KUHP) Musa Darwin Pane, Genesistha Endang Renika Siahaan," J. Din. Huk., vol. 26, no. 1, pp. 20–30, 2025, [Online]. Available: <https://www.unisbank.ac.id/ojs/index.php/fh1/article/view/10097/4247>
 - [8]. P. Chastro, T. Adensi, and O. Nasirun Indrasatya, "KAJIAN YURIDIS TERHADAP TRANSAKSI DIGITAL CRYPTOCURRENCY DARI PERSEPEKTIF PERLINDUNGAN KONSUMEN," J. Ilmu Hukum, Sos. dan Hum., vol. 3, no. 4, pp. 168–175, 2025, [Online]. Available: <https://jurnal.kolibi.id/index.php/kultura/article/view/114>
 - [9]. M. Ramadhan, "Illegal Access Melalui Metode Phishing pada Platform Transaksi Digital Cryptocurrency dalam Perspektif KUHP Baru dan UU ITE," 2026. [Online]. Available: <https://jurnal.umsb.ac.id/index.php/pagaruyuang/article/view/7142/4872>