JURRISH: Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora
Volume 5, Nomor 3, Juli 2026
E-ISSN .: 2828-7622; P-ISSN .: 2828-7630, Hal. 899-918
DOI: https://doi.org/10.55606/jurrish.v5i3.8643
Tersedia: https://prin.or.id/index.php/JURRISH

Analisis Yuridis Penggunaan *Cryptocurrency* sebagai Sarana Pendanaan Aksi Terorisme di Indonesia Beserta Tantangan dalam Penegakan Hukum

Rizky Dwi Utami[1]*, Ahmad Nafhani[2], Agung Pratama[3]
[1]Ilmu Hukum, Universitas Wira Buana, Indonesia
[2]Ilmu Hukum, Universitas Mulawarman, Indonesia
[3]Pengacara, Law Firm APR and Partners, Indonesia
Email : rizkydwiutamiutami11@gmail.com[1], ahmadnafhani@gmail.com[2], , agungpratama403@gmail.com[3]*
**Penulis Korespondensi: rizkydwiutami11@gmail.com*

Abstract. *The development of financial technology has led to the emergence of cryptocurrency as a decentralized digital instrument that enables fast and cross-border financial transactions. While this technology offers efficiency and flexibility in digital financial activities, it also creates opportunities for misuse in various forms of crime, including terrorist financing. This study aims to analyze the use of cryptocurrency as a means of financing terrorist activities in Indonesia, examine the existing legal framework governing terrorist financing, and identify the challenges faced in law enforcement. This research employs a normative legal method using statutory, conceptual, and case study approaches. The findings indicate that the use of cryptocurrency as a medium for terrorist financing still fulfills the elements of a criminal offense as regulated under Law Number 9 of 2013 concerning the Prevention and Eradication of Terrorism Financing. However, the characteristics of cryptocurrency, such as anonymity, decentralization, and cross-border transactions, create significant challenges in the processes of evidence gathering, transaction tracing, and identification of perpetrators. In addition, there is a regulatory gap between the recognition of crypto assets as economic commodities and the supervision of their potential misuse for terrorist financing. Therefore, stronger regulations are needed to explicitly integrate crypto assets into the terrorist financing prevention regime, along with improving the capacity of law enforcement agencies in blockchain transaction analysis and strengthening international cooperation to enhance the effectiveness of law enforcement in the digital economy era.*

Keywords: *Criminal Law; Crypto Assets; Cryptocurrency; Law Enforcement; Terrorist Financing.*

Perkembangan teknologi finansial telah melahirkan *cryptocurrency* sebagai instrumen digital yang beroperasi secara terdesentralisasi dan lintas batas negara. Di satu sisi, teknologi ini memberikan efisiensi dalam transaksi keuangan digital, namun di sisi lain membuka peluang penyalahgunaan untuk berbagai bentuk kejahatan, termasuk pendanaan terorisme. Penelitian ini bertujuan untuk menganalisis penggunaan *cryptocurrency* sebagai sarana pendanaan aksi terorisme di Indonesia, mengkaji pengaturan hukum yang berlaku, serta mengidentifikasi tantangan dalam penegakan hukumnya. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan peraturan perundang-undangan, pendekatan konseptual, dan pendekatan studi kasus. Hasil penelitian menunjukkan bahwa penggunaan *cryptocurrency* sebagai media pendanaan terorisme secara yuridis tetap memenuhi unsur tindak pidana sebagaimana diatur dalam Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme. Namun demikian, karakteristik *cryptocurrency* yang bersifat *pseudonim*, terdesentralisasi, dan lintas yurisdiksi menimbulkan berbagai hambatan dalam proses pembuktian, pelacakan transaksi, serta identifikasi pelaku. Selain itu, terdapat kesenjangan regulasi antara pengaturan aset kripto sebagai komoditas ekonomi dan pengawasan terhadap potensi penyalahgunaannya untuk pendanaan terorisme. Oleh karena itu, diperlukan penguatan regulasi yang secara eksplisit mengintegrasikan aset kripto ke dalam rezim pencegahan pendanaan terorisme, peningkatan kapasitas aparat penegak hukum dalam analisis transaksi blockchain, serta penguatan kerja sama internasional guna meningkatkan efektivitas penegakan hukum di era ekonomi digital.

Kata kunci: Aset Kripto; *Cryptocurrency*; Hukum Pidana; Pendanaan Terorisme; Penegakan Hukum.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah mendorong lahirnya berbagai inovasi di sektor keuangan yang dikenal sebagai *financial technology* (*fintech*). Salah satu manifestasi utama dari perkembangan tersebut adalah munculnya *cryptocurrency* sebagai instrumen digital berbasis kriptografi yang berfungsi sebagai sarana penyimpanan nilai, alat

Naskah Masuk: 15 Februari 2026; Revisi: 28 Februari 2026; Diterima: 13 Maret 2026;
Tersedia: 16 Maret 2026

pertukaran, dan objek investasi. *Cryptocurrency* beroperasi di atas teknologi *blockchain* yang memungkinkan pencatatan transaksi secara terdistribusi, transparan, serta tidak bergantung pada otoritas pusat. Karakteristik ini menjadikan *cryptocurrency* memiliki keunggulan berupa efisiensi, kecepatan transaksi, dan fleksibilitas lintas batas negara. Namun, di sisi lain, sifat terdesentralisasi dan pseudonim tersebut juga melahirkan potensi besar terhadap penyalahgunaan untuk berbagai tindak pidana berbasis teknologi informasi (Suhariyanto, 2013).

Perkembangan teknologi keuangan digital sejalan dengan perubahan pola kejahatan yang semakin bergeser dari bentuk konvensional menuju kejahatan berbasis digital (*cyber-enabled crime*). Kejahatan tidak lagi hanya dilakukan melalui pertemuan fisik dan sistem keuangan tradisional, melainkan memanfaatkan ruang siber sebagai medium utama. Pergeseran ini menunjukkan bahwa pelaku kejahatan bersifat adaptif terhadap perkembangan teknologi, sehingga hukum sebagai instrumen pengendali sosial dituntut untuk turut berkembang mengikuti dinamika tersebut (Marzuki, 2011). Dalam konteks ini, *cryptocurrency* menjadi salah satu instrumen yang kerap dimanfaatkan karena relatif sulit dilacak, dapat dipindahkan secara cepat, serta memungkinkan terjadinya transaksi lintas yurisdiksi tanpa melalui lembaga perantara konvensional.

Fenomena pendanaan terorisme merupakan salah satu bentuk kejahatan serius yang sangat bergantung pada dukungan finansial. Negara Indonesia merupakan negara berkembang dengan posisi yang sangat strategis memegang peranan penting di Asean menjadi salah satu sasaran terorisme. Setiap aktivitas terorisme, mulai dari perekrutan anggota, pelatihan, penyediaan logistik, propaganda, hingga pelaksanaan aksi, membutuhkan ketersediaan dana yang memadai. Oleh karena itu, pemutusan jalur pendanaan menjadi strategi kunci dalam pencegahan dan pemberantasan terorisme. Seiring berkembangnya teknologi, jaringan teroris tidak lagi semata-mata mengandalkan sistem perbankan konvensional, melainkan mulai memanfaatkan instrumen keuangan alternatif seperti *cryptocurrency*. *Financial Action Task Force* (FATF) bahkan menegaskan bahwa virtual assets memiliki risiko tinggi terhadap praktik pencucian uang dan pendanaan terorisme apabila tidak diatur melalui pendekatan berbasis risiko (*risk-based approach*) (Financial Action Task Force, 2014).

Di Indonesia, tindak pidana pendanaan terorisme telah diatur dalam Undang-Undang Nomor 9 Tahun 2013 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pendanaan Terorisme (2013), yang mengkriminalisasi setiap perbuatan menyediakan, mengumpulkan, memberikan, atau meminjamkan dana dengan tujuan digunakan untuk kegiatan terorisme. Namun demikian, pengaturan tersebut belum secara eksplisit mengatur penggunaan

cryptocurrency sebagai media pendanaan. Pada sisi lain, *cryptocurrency* justru diposisikan sebagai komoditas yang dapat diperdagangkan di bursa berjangka berdasarkan peraturan Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti), sementara Bank Indonesia melarang penggunaannya sebagai alat pembayaran yang sah. Kondisi ini menunjukkan adanya dualisme pendekatan, *cryptocurrency* diakui sebagai aset ekonomi, tetapi belum sepenuhnya terintegrasi ke dalam rezim pengawasan pendanaan terorisme (Assyamiri & Hardinanto, 2022).

Kesenjangan regulasi tersebut menimbulkan implikasi serius terhadap efektivitas penegakan hukum. Aparat penegak hukum menghadapi kesulitan dalam menelusuri identitas pemilik dompet digital, membuktikan keterkaitan antara transaksi kripto dan tujuan pendanaan terorisme, serta memperoleh data lintas negara yang berada di luar yurisdiksi Indonesia. Secara teoretis, pembuktian dalam hukum pidana menuntut adanya hubungan yang jelas antara perbuatan, pelaku, dan akibat yang ditimbulkan (Moeljatno, 2008). Ketika hubungan tersebut terfragmentasi oleh teknologi, maka penegakan hukum berpotensi menjadi tidak optimal. Untuk memberikan gambaran perbandingan antara sistem keuangan konvensional dan cryptocurrency dalam konteks risiko pendanaan terorisme, dapat dilihat pada tabel berikut:

Tabel 1. Perbandingan Sistem Keuangan Konvensional dan *Cryptocurrency.*

Aspek	Sistem Keuangan Konvensional	Cryptocurrency
Identitas Pengguna	Terikat KYC & bank	Pseudonim
Pengawasan	Terpusat	Terdesentralisasi
Kecepatan Transaksi	Relatif lambat	Sangat cepat
Lintas Negara	Melalui bank koresponden	Langsung
Risiko TF	Tinggi	Sangat tinggi

Berdasarkan uraian tersebut, tampak bahwa fenomena penggunaan *cryptocurrency* dalam pendanaan terorisme merupakan persoalan kompleks yang melibatkan aspek teknologi, ekonomi, dan hukum. Oleh karena itu, kajian hukum terhadap isu ini menjadi mendesak guna menjawab beberapa pertanyaan fundamental, yakni bagaimana praktik penggunaan *cryptocurrency* dalam pendanaan terorisme di Indonesia, bagaimana pengaturan hukum yang mengatur pendanaan terorisme dan relevansinya dengan *cryptocurrency,* serta bagaimana tantangan penegakan hukum terhadap pendanaan terorisme berbasis *cryptocurrency*. Jawaban atas pertanyaan-pertanyaan tersebut diharapkan dapat menjadi dasar perumusan kebijakan hukum yang adaptif dan responsif terhadap perkembangan teknologi finansial.

2. KAJIAN TEORITIS

Teori Negara Hukum (*Rule of Law*)

Konsep negara hukum menempatkan hukum sebagai dasar utama dalam penyelenggaraan kekuasaan negara. Dalam negara hukum, setiap tindakan pemerintah maupun masyarakat harus didasarkan pada aturan hukum yang berlaku. Prinsip ini bertujuan untuk menciptakan kepastian hukum, perlindungan hak asasi manusia, serta mencegah penyalahgunaan kekuasaan oleh pemerintah (Marzuki, 2011).

Dalam konteks penanggulangan terorisme, negara memiliki kewajiban untuk melindungi masyarakat dari ancaman yang dapat mengganggu keamanan nasional. Oleh karena itu, negara diberi kewenangan untuk membentuk regulasi yang mengatur berbagai bentuk kejahatan yang mengancam stabilitas negara, termasuk pendanaan terorisme. Kejahatan terorisme dipandang sebagai ancaman serius terhadap keamanan negara karena memiliki dampak luas terhadap ketertiban umum dan keselamatan masyarakat (Atmasasmita, 2003).

Perkembangan teknologi finansial seperti cryptocurrency menimbulkan tantangan baru bagi negara hukum karena transaksi keuangan dapat dilakukan secara anonim dan melintasi batas yurisdiksi negara. Kondisi ini menuntut negara untuk melakukan penyesuaian regulasi agar sistem hukum tetap mampu mengawasi aktivitas keuangan digital yang berpotensi digunakan untuk mendukung kejahatan, termasuk pendanaan terorisme.

Teori Kebijakan Hukum Pidana (*Criminal Policy*)

Kebijakan hukum pidana merupakan strategi yang digunakan oleh negara untuk menanggulangi kejahatan melalui penggunaan hukum pidana sebagai sarana pengendalian sosial. Kebijakan ini mencakup proses pembentukan norma hukum, penerapan hukum, serta upaya penegakan hukum yang bertujuan untuk melindungi masyarakat dari berbagai bentuk kejahatan (Wibowo, 2012).

Dalam kerangka kebijakan hukum pidana, penanggulangan terorisme dilakukan melalui pendekatan preventif dan represif. Pendekatan preventif bertujuan untuk mencegah terjadinya kejahatan sebelum terjadi, sedangkan pendekatan represif dilakukan melalui penindakan terhadap pelaku kejahatan setelah perbuatan tersebut terjadi. Pendanaan terorisme menjadi salah satu aspek yang sangat penting dalam upaya pencegahan terorisme karena keberadaan dana merupakan faktor utama yang memungkinkan jaringan teroris menjalankan aktivitasnya.

Seiring berkembangnya teknologi digital, pola pendanaan terorisme juga mengalami perubahan. Jaringan teroris tidak lagi hanya menggunakan sistem keuangan konvensional, tetapi mulai memanfaatkan instrumen keuangan digital seperti cryptocurrency yang memungkinkan perpindahan dana dilakukan secara cepat dan lintas negara. Hal ini menuntut

adanya kebijakan hukum pidana yang adaptif agar mampu menjangkau bentuk-bentuk kejahatan baru yang memanfaatkan perkembangan teknologi (Suhariyanto, 2013).

Teori Tindak Pidana (*Strafbaar Feit*)

Dalam hukum pidana, suatu perbuatan dapat dikategorikan sebagai tindak pidana apabila memenuhi unsur-unsur yang telah dirumuskan dalam undang-undang. Unsur-unsur tersebut meliputi adanya perbuatan yang dilarang oleh hukum, adanya kesalahan dari pelaku, serta adanya ancaman pidana yang mengatur perbuatan tersebut (Moeljatno, 2008). Pendanaan terorisme dalam sistem hukum Indonesia merupakan salah satu bentuk tindak pidana khusus yang diatur dalam Undang-Undang Nomor 9 Tahun 2013 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pendanaan Terorisme (2013). Delik ini menitikberatkan pada tindakan menyediakan, mengumpulkan, atau menyalurkan dana dengan tujuan untuk mendukung aktivitas terorisme.

Karakteristik penting dari tindak pidana pendanaan terorisme adalah bahwa delik ini termasuk dalam kategori tindak pidana formiil. Artinya, perbuatan menyediakan atau menyalurkan dana untuk kegiatan terorisme sudah dapat dipidana meskipun aksi terorisme yang didanai belum benar-benar terjadi. Pendekatan ini digunakan karena pendanaan dipandang sebagai tahap awal yang memungkinkan terlaksananya aksi terorisme.

Dalam konteks penggunaan *cryptocurrency*, aset digital dapat dipandang sebagai bentuk dana dalam arti luas selama memiliki nilai ekonomi dan dapat digunakan untuk mendukung aktivitas terorisme. Dengan demikian, penggunaan *cryptocurrency* sebagai sarana pendanaan terorisme tetap dapat dikualifikasikan sebagai tindak pidana sepanjang memenuhi unsur-unsur yang diatur dalam peraturan perundang-undangan.

Teori Pertanggungjawaban Pidana

Pertanggungjawaban pidana merupakan konsep yang menjelaskan bahwa seseorang hanya dapat dijatuhi pidana apabila terbukti melakukan kesalahan. Prinsip ini dikenal dengan asas geen straf zonder schuld, yang berarti tidak ada pidana tanpa kesalahan (Hamzah, 2012). Dalam perkara pendanaan terorisme, unsur kesengajaan menjadi faktor penting yang harus dibuktikan oleh aparat penegak hukum. Pelaku harus terbukti mengetahui bahwa dana yang disalurkannya akan digunakan untuk mendukung aktivitas terorisme. Apabila unsur kesengajaan tersebut dapat dibuktikan, maka pelaku dapat dimintai pertanggungjawaban pidana meskipun ia tidak terlibat secara langsung dalam pelaksanaan aksi terorisme.

Selain itu, hukum pidana juga mengenal konsep penyertaan yang memungkinkan lebih dari satu orang dimintai pertanggungjawaban atas suatu tindak pidana. Konsep ini mencakup pelaku utama, pihak yang turut serta melakukan kejahatan, serta pihak yang membantu

terjadinya kejahatan (Rusianto, 2016). Dalam konteks pendanaan terorisme berbasis cryptocurrency, pihak yang dapat dimintai pertanggungjawaban tidak hanya terbatas pada penyedia dana, tetapi juga dapat mencakup individu yang memfasilitasi transaksi atau membantu mengonversi dana ke dalam bentuk aset digital dengan tujuan mendukung aktivitas terorisme.

Teori Pembuktian dalam Hukum Pidana

Pembuktian merupakan tahap penting dalam proses penegakan hukum pidana karena menjadi dasar bagi hakim untuk menentukan apakah seseorang terbukti bersalah atau tidak. Dalam hukum pidana, pembuktian bertujuan untuk menunjukkan adanya hubungan antara perbuatan, pelaku, dan akibat yang ditimbulkan oleh suatu tindak pidana (Marzuki, 2011).
Dalam perkara pendanaan terorisme yang melibatkan *cryptocurrency*, proses pembuktian menghadapi tantangan yang cukup kompleks. Hal ini disebabkan oleh karakteristik teknologi *blockchain* yang bersifat pseudonim dan terdesentralisasi. Data transaksi yang tercatat dalam sistem *blockchain* hanya menunjukkan alamat dompet digital dan nilai transaksi tanpa secara langsung mengungkap identitas pemiliknya. Oleh karena itu, aparat penegak hukum perlu menggunakan pendekatan pembuktian yang lebih kompleks, termasuk melalui analisis forensik digital dan penelusuran transaksi blockchain. Selain itu, kerja sama internasional juga sering diperlukan karena transaksi *cryptocurrency* sering kali melibatkan platform atau server yang berada di luar yurisdiksi nasional.

3. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang bertujuan untuk mengkaji norma, asas, dan sistem hukum yang berkaitan dengan penggunaan *cryptocurrency* sebagai sarana pendanaan terorisme di Indonesia. Pendekatan yang digunakan meliputi pendekatan peraturan perundang-undangan (*statute approach*) dengan menelaah ketentuan dalam Undang-Undang Nomor 9 Tahun 2013 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pendanaan Terorisme (2013), Undang-Undang Nomor 5 Tahun 2018 Tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme (2018), serta regulasi terkait aset kripto, pendekatan konseptual (*conceptual approach*) dengan mengkaji doktrin dan teori hukum pidana serta hukum teknologi informasi, dan pendekatan studi kasus (*case approach*) melalui penelaahan temuan dan pengungkapan kasus penggunaan *cryptocurrency* dalam pendanaan terorisme di Indonesia.

4. HASIL DAN PEMBAHASAN

Penggunaan *Cryptocurrency* dalam Pendanaan Terorisme

Indikasi penggunaan *cryptocurrency* sebagai sarana pendanaan terorisme di Indonesia mulai mengemuka seiring dengan meningkatnya laporan transaksi keuangan mencurigakan yang dianalisis oleh Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). Dalam laporan tahunannya, PPATK menyebutkan bahwa sepanjang tahun 2022 ditemukan ratusan informasi terkait pendanaan kelompok teroris, dan sebagian di antaranya melibatkan pemanfaatan aset *kripto* sebagai media pemindahan dan penyamaran dana. Fenomena ini menunjukkan adanya adaptasi strategi oleh jaringan teroris yang sebelumnya lebih banyak menggunakan sistem perbankan konvensional, menjadi beralih pada instrumen keuangan digital yang relatif lebih sulit diawasi (Pusat Pelaporan dan Analisis Transaksi Keuangan, 2023).

Dalam salah satu pola yang diidentifikasi PPATK, dana awal diperoleh melalui pengumpulan donasi berkedok kegiatan sosial dan keagamaan, baik secara langsung maupun melalui platform digital. Dana tersebut kemudian dikonversi ke dalam bentuk *cryptocurrency* melalui layanan pertukaran aset kripto atau mekanisme transaksi *peer-to-peer*. Setelah dikonversi, dana tidak langsung dikirim ke pihak penerima akhir, melainkan dialirkan terlebih dahulu melalui beberapa dompet digital (wallet) yang berbeda. Perpindahan dana secara berlapis ini bertujuan untuk mengaburkan jejak transaksi dan mempersulit penelusuran asal-usul dana. Pada tahap akhir, dana kripto tersebut dikonversi kembali menjadi mata uang fiat atau digunakan secara langsung untuk mendanai kebutuhan operasional jaringan teroris, seperti pembelian peralatan, logistik, maupun pembiayaan perjalanan anggota (Financial Action Task Force, 2014).

Temuan PPATK tersebut memperoleh penguatan melalui pengungkapan kasus oleh Densus 88 Antiteror Polri pada Desember 2023. Dalam pengungkapan tersebut, aparat menemukan adanya aliran dana terorisme melalui transaksi *cryptocurrency* dengan nilai yang dilaporkan mencapai sekitar enam miliar rupiah. Dana tersebut diduga digunakan untuk mendukung aktivitas jaringan teroris, termasuk persiapan aksi dan kebutuhan logistik (Detik News, 2026). Pengungkapan ini memperlihatkan bahwa *cryptocurrency* tidak hanya berfungsi sebagai instrumen spekulasi ekonomi, tetapi juga telah dimanfaatkan secara nyata sebagai sarana kejahatan serius yang mengancam keamanan nasional.

Secara yuridis, kedua temuan tersebut memperlihatkan bahwa penggunaan *cryptocurrency* dalam pendanaan terorisme tetap memenuhi unsur tindak pidana sebagaimana dirumuskan dalam Undang-Undang Nomor 9 Tahun 2013, yakni adanya perbuatan

menyediakan, mengumpulkan, memberikan, atau meminjamkan dana dengan tujuan digunakan untuk kegiatan terorisme. Perbedaannya hanya terletak pada media yang digunakan, yaitu aset kripto, bukan uang tunai atau transfer bank. Dengan demikian, aspek media tidak menghapus sifat melawan hukum dari perbuatan pendanaan terorisme itu sendiri. Untuk memberikan gambaran yang lebih sistematis mengenai rekonstruksi pola kasus di Indonesia, berikut disajikan tabel ringkasan studi kasus:

Tabel 2. Rekonstruksi Studi Kasus Pendanaan Terorisme melalui *Cryptocurrency* di Indonesia.

No	Sumber Informasi	Sumber Dana Awal	Cara Konversi ke Kripto	Pola Transaksi	Tujuan Penggunaan
1	Temuan PPATK 2022	Donasi masyarakat, pengumpulan dana berkedok sosial	*Exchange kripto* / P2P	Transfer berlapis antar wallet, mixing	Logistik, perekrutan, dukungan jaringan
2	Densus 88 (2023)	Dana jaringan teroris	*Exchange kripto*	Pemindahan lintas wallet & lintas wilayah	Operasional & persiapan aksi

Sumber : pengolahan sumber berita detik.com, kompas, dan antara.

Studi kasus tersebut menunjukkan bahwa *cryptocurrency* berfungsi sebagai "lapisan pemutus" antara sumber dana dan tujuan akhir penggunaan dana. Hal ini berdampak langsung pada efektivitas pencegahan pendanaan terorisme, karena mekanisme pengawasan konvensional yang berbasis lembaga keuangan formal menjadi kurang optimal. Aparat penegak hukum dituntut untuk tidak hanya memahami aspek normatif hukum pidana, tetapi juga memiliki kapasitas teknis dalam menganalisis transaksi *blockchain* (Suhariyanto, 2013).

Dari perspektif kebijakan hukum, studi kasus ini menegaskan urgensi penguatan regulasi yang secara eksplisit mengintegrasikan aset kripto ke dalam rezim pencegahan pendanaan terorisme, baik melalui kewajiban pelaporan transaksi mencurigakan oleh penyedia jasa aset kripto, peningkatan koordinasi antara PPATK, aparat penegak hukum, dan otoritas pengawas perdagangan aset kripto, maupun penguatan kerja sama internasional. Tanpa langkah-langkah tersebut, penggunaan *cryptocurrency* berpotensi terus menjadi celah yang dimanfaatkan jaringan teroris untuk menyembunyikan dan memindahkan dana (Financial Action Task Force, 2012).

Analisis Yuridis Penggunaan *Cryptocurrency* dalam Pendanaan Terorisme

Pengaturan Hukum Pendanaan Terorisme dan Relevansinya dengan Cryptocurrency

Pengaturan mengenai pendanaan terorisme di Indonesia secara khusus diatur dalam Undang-Undang Nomor 9 Tahun 2013 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pendanaan Terorisme (2013) yang dalam hal ini di sebut Undang-Undang Nomor 9 Tahun 2013. Undang-undang ini lahir sebagai bentuk komitmen Indonesia dalam mengimplementasikan International *Convention for the Suppression of the Financing of Terrorism* 1999 serta menyesuaikan diri dengan standar internasional pencegahan pencucian uang dan pendanaan terorisme.

Secara normatif, Pasal 4 Undang-Undang Nomor 9 Tahun 2013 merumuskan *bahwa setiap orang yang dengan sengaja menyediakan, mengumpulkan, memberikan, atau meminjamkan dana, baik secara langsung maupun tidak langsung, dengan maksud digunakan untuk melakukan tindak pidana terorisme, dipidana dengan ancaman penjara paling lama lima belas tahun dan denda paling banyak satu miliar rupiah*.

Ketentuan ini menegaskan bahwa fokus kriminalisasi terletak pada unsur perbuatan menyediakan atau mengalirkan dana dan adanya tujuan untuk mendukung aktivitas terorisme, bukan pada bentuk atau media dana tersebut. Dengan demikian, secara teoritis, penggunaan *cryptocurrency* sebagai media transfer dana tetap berada dalam cakupan norma tersebut sepanjang terpenuhi unsur kesengajaan dan tujuan pendanaan terorisme.

Selain itu, Undang-Undang Nomor 9 Tahun 2013 juga memberikan kewenangan yang luas kepada Aparat Penegak Hukum untuk melakukan pemblokiran dan penyitaan terhadap dana yang diduga terkait dengan aktivitas terorisme. Mekanisme ini dimaksudkan untuk memutus aliran dana sebelum dana tersebut digunakan untuk mendukung aksi teror. Dalam perspektif hukum pidana, kebijakan tersebut mencerminkan pendekatan preventif dan represif sekaligus, karena negara tidak hanya menunggu terjadinya aksi teror, tetapi juga berupaya mencegahnya melalui pemutusan jalur pendanaan (Wibowo, 2012). Namun, ketika dana yang dimaksud berbentuk *cryptocurrency*, pelaksanaan kewenangan pemblokiran dan penyitaan menjadi lebih kompleks, mengingat dompet digital dapat berada di luar yurisdiksi nasional dan tidak selalu berada di bawah kendali lembaga keuangan formal.

Pengaturan mengenai tindak pidana terorisme sendiri diperbarui melalui Undang-Undang Nomor 5 Tahun 2018 yang merupakan perubahan atas Undang-Undang Nomor 15 Tahun 2003. Undang-Undang ini memperluas definisi terorisme, mempertegas kewenangan aparat penegak hukum dan kelembagaan dibawah pemerintah dalam mengatasi aksi terorisme, serta memperkuat aspek pencegahan melalui pendekatan deradikalisasi dan pelibatan berbagai

institusi negara. Dalam konteks pendanaan, Undang-Undang Nomor 5 Tahun 2018 mempertegas keterkaitan antara pelaku utama dan pihak yang membantu, termasuk mereka yang menyediakan dukungan finansial. Secara sistemik, kedua undang-undang tersebut membentuk rezim hukum khusus (*lex specialis*) yang berdiri di luar KUHP, dengan karakteristik penanganan yang berbeda dari tindak pidana umum meskipun saat ini terkait tindak pidana terorisme juga sedikit di atur di dalam Pasal 600 s.d. 602 KUHP yang ada dalam Undang-Undang Nomor 1 Tahun 2023 sebagaimana telah disesuaikan kembali ke dalam Undang-Undang Nomor 1 Tahun 2026. Akan tetapi, aturan undang-undang tersebut belum secara eksplisit menyebut atau mengatur penggunaan *cryptocurrency* sebagai instrumen pendanaan terorisme, sehingga interpretasi normatif masih bergantung pada konstruksi "dana" dalam arti luas.

Di sisi lain, status hukum *cryptocurrency* di Indonesia diatur melalui pendekatan yang berbeda. *Cryptocurrency* tidak diakui sebagai alat pembayaran yang sah berdasarkan Undang-Undang Nomor 7 Tahun 2011 Tentang Mata Uang Dan Peraturan Bank Indonesia (2011), melainkan diposisikan sebagai komoditas yang dapat diperdagangkan di bursa berjangka berdasarkan regulasi Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) (Assyamiri & Hardinanto, 2022). Dengan demikian, negara mengakui eksistensi *cryptocurrency* dalam ranah ekonomi, tetapi belum sepenuhnya mengintegrasikannya ke dalam kerangka pengawasan keamanan nasional, khususnya dalam konteks pencegahan pendanaan terorisme. Untuk memahami posisi tersebut secara lebih sistematis, berikut tabel perbandingan kerangka regulasi yang berlaku:

Tabel 3. Perbandingan Kerangka Regulasi yang Berlaku.

Aspek	Undang-Undang Nomor 9 Tahun 2013	Undang-Undang Nomor 5 Tahun 2018	Regulasi Kripto (Bappebti)
Fokus	Pendanaan terorisme	Tindak pidana terorisme	Perdagangan aset kripto
Subjek Hukum	Penyedia/penyalur dana	Pelaku teror & pendukung	Pedagang & konsumen kripto
Instrumen Pengawasan	Pemblokiran & penyitaan dana	Penangkapan & penindakan	Pengawasan transaksi perdagangan
Pengaturan Kripto	Tidak eksplisit	Tidak eksplisit	Diakui sebagai komoditas

Tabel tersebut memperlihatkan adanya fragmentasi pengaturan antara rezim keamanan dan rezim ekonomi digital. Kesenjangan regulasi ini menimbulkan tantangan dalam praktik, karena aparat penegak hukum harus menafsirkan norma umum mengenai "dana" untuk mencakup aset kripto, sementara mekanisme pengawasan perdagangan kripto tidak selalu

dirancang untuk mendeteksi risiko pendanaan terorisme. Dalam perspektif teori hukum, kondisi ini dapat dikategorikan sebagai regulatory lag, yaitu keterlambatan regulasi dalam merespons perkembangan teknologi (Marzuki, 2011).

Jika dibandingkan dengan standar internasional yang dirumuskan oleh *Financial Action Task Force* (FATF), negara-negara anggota diwajibkan untuk memastikan bahwa *virtual asset service providers* (VASPs) tunduk pada kewajiban know your customer, pelaporan transaksi mencurigakan, dan mekanisme kerja sama internasional. FATF *Recommendation* secara khusus menekankan pentingnya pengawasan terhadap penyedia jasa aset virtual sebagai bagian dari rezim anti-*money laundering* dan *counter-terrorism financing* (Financial Action Task Force, 2012). Dalam konteks ini, Indonesia telah mulai mengadopsi pendekatan tersebut melalui kewajiban pelaporan oleh penyedia jasa aset kripto kepada PPATK, namun integrasi penuh antara rezim perdagangan dan rezim keamanan masih memerlukan penguatan.

Secara keseluruhan, pengaturan hukum pendanaan terorisme di Indonesia telah memiliki fondasi normatif yang kuat melalui Undang-Undang Nomor 9 Tahun 2013 dan Undang-Undang Nomor 5 Tahun 2018, tetapi relevansinya dengan perkembangan cryptocurrency masih memerlukan interpretasi progresif dan reformulasi kebijakan. Tanpa integrasi yang lebih sistematis antara regulasi aset kripto dan rezim pencegahan pendanaan terorisme, potensi penyalahgunaan *cryptocurrency* akan tetap menjadi celah dalam sistem hukum nasional. Oleh karena itu, harmonisasi regulasi dan penguatan pengawasan terhadap transaksi aset kripto menjadi kebutuhan mendesak dalam menjaga stabilitas keamanan nasional di era ekonomi digital.

Penggunaan *cryptocurrency* sebagai sarana pendanaan terorisme menimbulkan persoalan penting dalam kualifikasi tindak pidana, khususnya terkait bagaimana perbuatan tersebut ditempatkan dalam sistem hukum pidana nasional. Secara konseptual, kualifikasi tindak pidana merupakan proses penggolongan suatu perbuatan ke dalam kategori delik tertentu berdasarkan unsur-unsur yang dirumuskan dalam undang-undang.

Dalam konteks pendanaan terorisme, Undang-Undang Nomor 9 Tahun 2013 menegaskan bahwa setiap orang yang dengan sengaja menyediakan, mengumpulkan, memberikan, atau meminjamkan dana, baik secara langsung maupun tidak langsung, dengan maksud digunakan untuk melakukan tindak pidana terorisme, organisasi teroris, atau teroris, dipidana sebagai pelaku tindak pidana pendanaan terorisme. Rumusan tersebut menempatkan fokus utama pada perbuatan dan tujuan penggunaan dana, bukan pada bentuk atau jenis media yang digunakan. Oleh karena itu, *cryptocurrency* sebagai bentuk aset digital dapat

dikualifikasikan sebagai "dana" dalam arti luas, sepanjang memiliki nilai ekonomi dan dapat digunakan untuk mendukung aktivitas terorisme.

Dari sudut pandang hukum pidana, penggunaan *cryptocurrency* dalam pendanaan terorisme dapat dikualifikasikan sebagai tindak pidana formil, karena undang-undang menitikberatkan pada perbuatan menyediakan atau menyalurkan dana dengan maksud tertentu, tanpa mensyaratkan terjadinya akibat berupa terlaksananya aksi terorisme. Selain itu, perbuatan tersebut juga dapat digolongkan sebagai tindak pidana sengaja (dolus), mengingat unsur kesengajaan menjadi elemen utama dalam rumusan pasal. Dengan demikian, sepanjang dapat dibuktikan bahwa pelaku mengetahui dan menghendaki dana yang disalurkannya digunakan untuk kepentingan terorisme, maka unsur subjektif tindak pidana telah terpenuhi (Moeljatno, 2008).

Lebih lanjut, kualifikasi tindak pidana ini juga berkaitan dengan doktrin *extraordinary crime*, yang menempatkan terorisme dan pendanaannya sebagai kejahatan luar biasa karena mengancam keamanan negara, ketertiban umum, serta hak asasi manusia, khususnya hak untuk hidup. Oleh karena itu, negara diberikan kewenangan yang lebih luas untuk melakukan tindakan preventif dan represif, termasuk pemblokiran aset, penyitaan, serta penindakan terhadap pihak-pihak yang terlibat, baik sebagai pelaku utama maupun sebagai pembantu (Atmasasmita, 2003). Dalam konteks *cryptocurrency*, pendekatan ini menegaskan bahwa meskipun teknologi yang digunakan bersifat baru, substansi kejahatan tetap berada dalam kerangka kejahatan luar biasa yang harus ditangani secara tegas.

Pertanggungjawaban Pidana Pelaku

Pertanggungjawaban pidana dalam hukum pidana Indonesia didasarkan pada asas geen straf zonder schuld, yang berarti tidak ada pidana tanpa kesalahan. Artinya, seseorang hanya dapat dimintai pertanggungjawaban pidana apabila dapat dibuktikan adanya kesalahan dalam bentuk kesengajaan atau kealpaan, serta kemampuan bertanggung jawab. Dalam tindak pidana pendanaan terorisme berbasis cryptocurrency, pertanggungjawaban pidana pelaku melekat pada siapa pun yang secara sadar dan sengaja terlibat dalam penyediaan, pengumpulan, atau penyaluran dana melalui aset kripto untuk tujuan terorisme (Rusianto, 2016).

Negara Indonesia merupakan negara berkembang dengan posisi yang sangat strategis memegang peranan penting di Asean menjadi salah satu sasaran terorisme. Berdasarkan data laporan *Global Terrorism Index* (GTI) tahun 2024, Indonesia mengalami perbaikan situasi keamanan yang ditandai dengan turunnya peringkat dari 24 menjadi 31. Hal tersebut dianggap sebagai suatu status peningkatan di karenakan di tahun 2022 dan 2023, Indonesia masih dalam posisi peringkat 24 dalam laporan *Global Terrorism Index*. Serta

perubahan status dari *Medium Impacted* menjadi *Low Impacted* terdampak terrorisme (Laporan Pers Silis BNPT; 2024). Dan menurut laporan *Global Peace Index* (GPI) tahun 2024, Indonesia juga mengalami kenaikan 5 peringkat dari 53 ke 48, sehingga Indonesia masih menyandang predikat *high peace country*. Dan yang terakhir, bedasarkan hasil evaluasi Indeks Risiko Terorisme (IRT), terdapat beberapa data yang menyatakan nilai risiko daerah menjadi target serangan maupun penyuplai teror dari tahun 2021 s.d. 2023 (BNPT; 2023).

Tabel 4. Data Indeks Risiko Terorisme (IRT) Tahun 2021 s.d. 2023.

No	Tahun	Dimensi Target Daerah	Dimensi Suplai Pelaku
1	2021	52,22%	30,29%
2	2022	51,54%	29,48%
3	2023	51,97%	30,01%

Sumber : Laporan Kinerja Badan Nasional Penanggulangan Terorisme, 2023

Berdasarkan data GTI, GPI dan IRT tersebut diatas, disimpulkan periode turun naiknya skala kerawanan, Indonesia masih tergolong ke dalam negara dengan tingkat perdamaian yang tinggi. Namun dengan turun naiknya angka serangan aksi terorisme yang ada dalam hasil IRT di tahun 2021 s.d. 2023, bukan berarti aksi terorisme berhenti secara permukaan. Tindak Pidana Terorisme pada dasarnya bersifat transnasional dan terorganisasi karena memiliki kekhasan yang bersifat klandestin yaitu rahasia, diam-diam, atau gerakan bawah tanah, lintas negara yang didukung oleh pendayagunaan teknologi modern di bidang komunikasi, informatika, transportasi, dan persenjataan modern sehingga memerlukan kerjasama di tingkat international untuk menanggulanginya.

Pelaku dalam konteks ini tidak hanya terbatas pada aktor utama yang menginisiasi pendanaan, tetapi juga mencakup pihak-pihak yang turut serta (*medepleger)*, membantu (*medeplichtige*), atau melakukan permufakatan jahat. Dengan demikian, operator platform ilegal, perantara transaksi, maupun individu yang memfasilitasi konversi dana ke dalam *cryptocurrency* dapat dimintai pertanggungjawaban pidana sepanjang terbukti mengetahui tujuan penggunaan dana tersebut. Hal ini sejalan dengan doktrin penyertaan dalam hukum pidana, yang mengakui bahwa setiap orang yang berkontribusi terhadap terwujudnya tindak pidana dapat dimintai pertanggungjawaban sesuai dengan perannya (Hamzah, 2012).

Dalam perspektif kebijakan hukum pidana, pertanggungjawaban pidana terhadap pelaku pendanaan terorisme berbasis *cryptocurrency* juga mencerminkan orientasi perlindungan kepentingan publik dan keamanan nasional. Negara tidak hanya berupaya menghukum pelaku setelah terjadinya aksi teror, tetapi juga mencegah terjadinya aksi tersebut dengan

mengkriminalisasi seluruh rangkaian pendanaan. Dengan demikian, pertanggungjawaban pidana berfungsi sebagai instrumen pencegahan umum *(general prevention*) dan pencegahan khusus (*special prevention*).

Hambatan Pembuktian dan Penegakan Hukum

Hambatan pembuktian dalam perkara pendanaan terorisme berbasis *cryptocurrency* pada dasarnya berangkat dari karakter teknologi *blockchain* itu sendiri yang bersifat pseudonim, terdesentralisasi, dan lintas batas negara. Meskipun setiap transaksi tercatat secara permanen dalam distributed ledger, data yang terekam hanya berupa alamat dompet digital dan nilai transaksi, tanpa secara otomatis memuat identitas hukum pemiliknya. Kondisi ini berbeda secara fundamental dengan sistem perbankan konvensional yang mewajibkan penerapan prinsip mengenali pengguna jasa (*know your customer*/KYC) dan pelaporan transaksi mencurigakan. Akibatnya, aparat penegak hukum menghadapi kesulitan awal dalam mengaitkan suatu alamat dompet dengan subjek hukum tertentu, sehingga proses pembuktian tidak dapat langsung diarahkan kepada individu atau kelompok yang diduga sebagai pelaku. Dalam perspektif teori pembuktian hukum pidana, pembuktian harus mampu menunjukkan hubungan kausal antara perbuatan, pelaku, dan tujuan tindak pidana. Ketika hubungan tersebut terfragmentasi oleh teknologi, maka konstruksi pembuktian menjadi jauh lebih kompleks (Marzuki, 2011).

Selain persoalan identifikasi pelaku, hambatan pembuktian juga muncul dari penggunaan teknik layering dalam transaksi *cryptocurrency*. Pelaku pendanaan terorisme kerap memindahkan dana melalui banyak dompet digital, menggunakan layanan *mixing* atau *tumbler*, serta melakukan pertukaran antarjenis kripto (*coin swapping*) untuk mengaburkan jejak transaksi. Teknik-teknik tersebut pada dasarnya mereplikasi pola pencucian uang konvensional, namun dengan tingkat kompleksitas yang lebih tinggi karena memanfaatkan teknologi kriptografi. Dalam praktiknya, aparat penegak hukum memerlukan keahlian forensik digital dan perangkat lunak khusus untuk menganalisis pola transaksi blockchain, sementara kapasitas tersebut belum merata di seluruh institusi penegak hukum di Indonesia (Suhariyanto, 2013).

Hambatan berikutnya berkaitan dengan aspek yurisdiksi. Transaksi cryptocurrency bersifat lintas batas dan sering kali melibatkan platform pertukaran aset kripto yang berkedudukan di luar negeri. Untuk memperoleh data transaksi atau identitas pengguna, aparat penegak hukum harus menempuh mekanisme kerja sama internasional, baik melalui mutual legal assistance maupun jalur informal antarlembaga. Proses ini sering kali memakan waktu lama dan bergantung pada kesediaan negara lain untuk memberikan bantuan, sehingga

berdampak pada lambatnya penanganan perkara. Dalam konteks kejahatan terorisme yang bersifat cepat dan dinamis, keterlambatan tersebut berpotensi mengurangi efektivitas pencegahan (Wibowo, 2012).

Dari sisi penegakan hukum, hambatan juga muncul akibat belum adanya pengaturan teknis yang komprehensif mengenai tata cara penyitaan, pengelolaan, dan perampasan aset kripto sebagai barang bukti. Meskipun Undang-Undang Nomor 9 Tahun 2013 memberikan kewenangan pemblokiran dan penyitaan dana yang diduga terkait pendanaan terorisme, implementasi terhadap aset kripto masih memerlukan penafsiran progresif. Aparat penegak hukum harus memastikan bahwa proses penyitaan tidak hanya sah secara hukum, tetapi juga aman secara teknis, mengingat pengelolaan dompet digital memerlukan penguasaan kunci privat (*private key*) yang bersifat sangat sensitif. Tanpa pedoman teknis yang jelas, terdapat risiko hilangnya aset atau tidak optimalnya pemanfaatan aset sitaan untuk kepentingan pembuktian. Untuk memberikan gambaran ringkas mengenai hambatan utama tersebut, berikut tabel ringkasan:

Tabel 5. Hambatan Penegakan Hukum.

Aspek	Bentuk Hambatan	Dampak
Identitas pelaku	Pseudonim wallet	Sulit menentukan subjek hukum
Yurisdiksi	Server & platform di luar negeri	Proses hukum lambat
Teknis	Keterbatasan forensik blockchain	Bukti sulit dibangun
Regulasi	Belum spesifik mengatur kripto dalam TF	Celah hukum

Hambatan-hambatan tersebut menunjukkan bahwa penegakan hukum terhadap pendanaan terorisme berbasis *cryptocurrency* tidak dapat hanya mengandalkan mekanisme konvensional, melainkan memerlukan pendekatan multidisipliner yang menggabungkan hukum, teknologi informasi, dan kerja sama internasional.

Reformulasi kebijakan hukum atau ius constituendum dalam konteks pendanaan terorisme berbasis *cryptocurrency* harus diarahkan pada upaya mempersempit celah hukum yang muncul akibat perkembangan teknologi finansial. Secara normatif, Indonesia telah memiliki fondasi yang kuat melalui Undang-Undang Nomor 9 Tahun 2013 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pendanaan Terorisme (2013) serta Undang-Undang Nomor 5 Tahun 2018 Tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme (2018). Namun, kedua undang-undang tersebut belum secara eksplisit mengatur posisi *cryptocurrency* sebagai instrumen pendanaan, sehingga diperlukan penguatan norma yang secara tegas memasukkan aset kripto ke dalam cakupan objek pengawasan pendanaan terorisme.

Reformulasi pertama yang mendesak adalah penegasan definisi "dana" dalam undang-undang pendanaan terorisme agar mencakup aset digital dan virtual assets. Penegasan ini penting untuk menghilangkan keraguan interpretatif dan memberikan kepastian hukum bagi aparat penegak hukum dalam menindak pelaku. Selain itu, perlu dibangun kerangka kewajiban yang jelas bagi penyedia jasa aset kripto untuk menerapkan prinsip KYC, pelaporan transaksi mencurigakan, serta kewajiban kerja sama dengan PPATK dan aparat penegak hukum. Pendekatan ini sejalan dengan rekomendasi *Financial Action Task Force (FATF)* yang mewajibkan negara anggota untuk mengawasi *virtual asset service providers* sebagai bagian dari *rezim anti-money laundering* dan *counter-terrorism financing* (Financial Action Task Force, 2012). Reformulasi berikutnya berkaitan dengan penguatan kapasitas institusional. Negara perlu mengembangkan unit khusus atau memperkuat unit yang sudah ada dalam hal forensik *blockchain*, baik di lingkungan kepolisian, kejaksaan, maupun PPATK. Penguatan ini mencakup pelatihan sumber daya manusia, pengadaan perangkat lunak analisis *blockchain*, serta penyusunan standar operasional prosedur penanganan barang bukti kripto. Dengan demikian, proses pembuktian dapat dilakukan secara lebih sistematis dan akuntabel.

Di samping itu, reformulasi kebijakan hukum juga harus menyentuh aspek kerja sama internasional. Mengingat transaksi *cryptocurrency b*ersifat lintas batas, Indonesia perlu memperluas perjanjian kerja sama dan mekanisme pertukaran informasi dengan negara lain serta dengan penyedia platform global. Kerja sama ini menjadi kunci untuk mempercepat penelusuran transaksi dan pemblokiran aset yang berada di luar yurisdiksi nasional.

Secara keseluruhan, reformulasi kebijakan hukum dalam konteks pendanaan terorisme berbasis *cryptocurrency* harus diarahkan pada integrasi antara rezim keamanan nasional dan rezim ekonomi digital. Hukum tidak lagi dapat memandang aset kripto semata-mata sebagai komoditas perdagangan, tetapi juga sebagai instrumen yang berpotensi digunakan untuk kejahatan serius. Dengan pendekatan tersebut, sistem hukum nasional diharapkan mampu merespons perkembangan teknologi secara adaptif sekaligus tetap menjamin perlindungan terhadap keamanan negara dan masyarakat.

5. KESIMPULAN

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa penggunaan *cryptocurrency* sebagai sarana pendanaan aksi terorisme di Indonesia merupakan fenomena yang nyata dan bukan sekadar potensi teoretis. Karakteristik *cryptocurrency* yang bersifat terdesentralisasi, pseudonim, dan lintas batas menjadikannya instrumen yang rentan disalahgunakan oleh jaringan terorisme untuk menyamarkan dan memindahkan dana. Meskipun secara normatif

Undang-Undang Nomor 9 Tahun 2013 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pendanaan Terorisme (2013) telah memberikan dasar hukum yang cukup untuk menjerat pelaku, pengaturan tersebut belum secara eksplisit mengintegrasikan aset kripto ke dalam rezim pengawasan pendanaan terorisme. Akibatnya, aparat penegak hukum menghadapi berbagai hambatan dalam aspek pembuktian, identifikasi pelaku, serta pelacakan aliran dana yang melibatkan teknologi *blockchain* dan yurisdiksi lintas negara.

Selain itu, terdapat kesenjangan regulasi antara pendekatan keamanan nasional dan pendekatan ekonomi digital dalam pengaturan *cryptocurrency* di Indonesia. Di satu sisi, aset kripto diakui sebagai komoditas yang dapat diperdagangkan, namun di sisi lain belum sepenuhnya diharmonisasikan dengan sistem pencegahan pendanaan terorisme. Kondisi ini menunjukkan bahwa sistem hukum nasional masih berada dalam fase adaptasi terhadap perkembangan teknologi finansial. Oleh karena itu, diperlukan langkah strategis yang mampu mengintegrasikan perkembangan teknologi dengan kebutuhan perlindungan keamanan negara, tanpa menghambat inovasi ekonomi digital secara proporsional.

Saran

Pertama, diperlukan penguatan regulasi melalui reformulasi norma dalam undang-undang pendanaan terorisme agar secara eksplisit mencakup aset kripto dan bentuk virtual assets lainnya sebagai objek pengawasan. Penegasan ini penting untuk memberikan kepastian hukum dan menghindari perdebatan interpretatif dalam proses penegakan hukum. Selain itu, pemerintah perlu memastikan bahwa seluruh penyedia jasa aset kripto menerapkan prinsip know your customer, pelaporan transaksi mencurigakan, serta kerja sama aktif dengan PPATK dan aparat penegak hukum sebagai bagian dari rezim pencegahan pendanaan terorisme.

Kedua, negara perlu meningkatkan kapasitas institusional dan teknis aparat penegak hukum dalam bidang forensik digital dan analisis blockchain, serta memperkuat kerja sama internasional dalam pelacakan transaksi lintas batas. Penguatan sumber daya manusia, pengadaan teknologi pendukung, dan penyusunan pedoman teknis penanganan barang bukti kripto menjadi langkah strategis untuk memastikan efektivitas pembuktian di pengadilan. Dengan pendekatan yang terintegrasi antara regulasi, teknologi, dan kerja sama global, sistem hukum Indonesia diharapkan mampu merespons secara adaptif dan efektif terhadap tantangan pendanaan terorisme di era ekonomi digital.

DAFTAR REFERENSI

Adams, S., Scherer, W. T., & Beling, P. A. (2017). Data, insights, models, and decisions: Machine learning in context. In *Intuition, trust, and analytics*. https://doi.org/10.1201/9781315195551

Alamouti, S. M., Arjomandi, F., Burger, M., & Gün, H. (2026). Device first continuum AI (DFC-AI): Realizing human-like AI. *Lecture Notes in Networks and Systems, 1676*, 482–495. https://doi.org/10.1007/978-3-032-07989-3_31

Altingovde, I. S., Cambazoglu, B. B., & Tonellotto, N. (2015). LSDS-IR'15: 2015 workshop on large-scale and distributed systems for information retrieval. *Proceedings of the International Conference on Information and Knowledge Management*, 1947–1948. https://doi.org/10.1145/2806416.2806877

Anand, A. S., Sawant, S., Reinhardt, D. P., & Gros, S. (2025). Predicting what matters: Training AI models for better decisions. *IEEE Transactions on Neural Networks and Learning Systems*. https://doi.org/10.1109/TNNLS.2025.3633573

Barreiro-Gomez, J., Ocampo-Martinez, C., & Quijano, N. (2017). Partitioning for large-scale systems: A sequential distributed MPC design. *IFAC-PapersOnLine, 50*(1), 8838–8843. https://doi.org/10.1016/j.ifacol.2017.08.1539

Bilal, H., Rehman, A., Aslam, M. S., Ullah, I., Chang, W.-J., Kumar, N., & Almuhaideb, A. M. (2025). Hybrid TrafficAI: A generative AI framework for real-time traffic simulation and adaptive behavior modeling. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2025.3571041

Cabrera, O., Franch, X., & Marco, J. (2017). Ontology-based context modeling in service-oriented computing: A systematic mapping. *Data and Knowledge Engineering, 110*, 24–53. https://doi.org/10.1016/j.datak.2017.03.008

Cinque, M., Cotroneo, D., Esposito, C., Fiorentino, M., & Russo, S. (2018). Designing resilient and secure large-scale crisis information systems. In *Volatiles in the Martian crust*. https://doi.org/10.1016/B978-0-12-811373-8.00014-8

Costa, F. S. (2025). Three ways industrial AI enhances traditional control systems. *Control Engineering, 72*(6), 26–27.

Dai, H., Wang, Y., Kent, K. B., Zeng, L., & Xu, C. (2022). The state of the art of metadata managements in large-scale distributed file systems: Scalability, performance and availability. *IEEE Transactions on Parallel and Distributed Systems, 33*(12), 3850–3869. https://doi.org/10.1109/TPDS.2022.3170574

De Luca, E. W., Said, A., Crestani, F., & Elsweiler, D. (2015). 5th workshop on context-awareness in retrieval and recommendation. *Lecture Notes in Computer Science, 9022*, 830–833. https://doi.org/10.1007/978-3-319-16354-3_96

Fujimaki, R., Muraoka, Y., Ito, S., & Yabe, A. (2016). From prediction to decision making: Predictive optimization technology. *NEC Technical Journal, 11*(1), 62–65.

Haroon, M., Siddiqui, Z. A., Husain, M., Ali, A., & Ahmad, T. (2024). A proactive approach to fault tolerance using predictive machine learning models in distributed systems. *International Journal of Experimental Research and Review, 44*, 208–220. https://doi.org/10.52756/ijerr.2024.v44spl.018

Karadayi-Usta, S. (2024). Fuzzy rule-based systems: How to construct a FRBS with MATLAB, R, and Python. In *Decision-making models: A perspective of fuzzy logic and machine learning*. https://doi.org/10.1016/B978-0-443-16147-6.00008-6

Khan, M. T., Durrani, M., Khalid, S., & Aziz, F. (2016). Lifelong aspect extraction from big data: Knowledge engineering. *Complex Adaptive Systems Modeling, 4*(1). https://doi.org/10.1186/s40294-016-0018-7

Kumar, V. S., Antony, S., Rao, R., Anitha, B., Prasad, B. V. V. S., & Maram, B. (2025). Artificial intelligence and optimization: Perfecting decision-making models. *Proceedings of the 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS 2025)*, 1195–1200. https://doi.org/10.1109/ICSCDS65426.2025.11167208

Legrand, I. C. (2016). Monitoring and control of large-scale distributed systems. *Proceedings of the International School of Physics "Enrico Fermi," 192*, 101–151. https://doi.org/10.3254/978-1-61499-643-9-101

Liu, H., Gegov, A., & Cocea, M. (2016). Introduction. *Studies in Big Data, 13*, 1–9. https://doi.org/10.1007/978-3-319-23696-4_1

Machado, R., Rosa, F., Almeida, R., Primo, T., Pilla, M., Pernas, A., & Yamin, A. (2018). A hybrid architecture to enrich context awareness through data correlation. *Proceedings of the ACM Symposium on Applied Computing*, 1451–1453. https://doi.org/10.1145/3167132.3167405

Palivela, L. H., Vivekanandan, D., Chinniah, P., Kiranbabu, M. N. V., Panneer Dhas, L., Srivastava, P., & Anantraj, I. (2024). Revolutionizing AI decision-making with hybrid rule-based systems: A novel framework for transparent and accurate outcomes. *Communications on Applied Nonlinear Analysis, 31*(8S), 115–127. https://doi.org/10.52783/cana.v31.1460

Pierson, J.-M., & Hlavacs, H. (2015). Introduction to energy efficiency in large-scale distributed systems. In *Large-scale distributed systems and energy efficiency: A holistic view*. https://doi.org/10.1002/9781118981122.ch1

Pushpa, P. V. (2017). Customer context based transactions in mobile commerce business environment. *Proceedings of the 13th IEEE International Conference on E-Business Engineering*, 208–213. https://doi.org/10.1109/ICEBE.2016.043

Quijano, N., Ocampo-Martinez, C., Barreiro-Gomez, J., Obando, G., Pantoja, A., & Mojica-Nava, E. (2017). The role of population games and evolutionary dynamics in distributed control systems: The advantages of evolutionary game theory. *IEEE Control Systems, 37*(1), 70–97. https://doi.org/10.1109/MCS.2016.2621479

Rocha, R. R., Oliveira-Lopes, L. C., & Christofides, P. D. (2018). Partitioning for distributed model predictive control of nonlinear processes. *Chemical Engineering Research and Design, 139*, 116–135. https://doi.org/10.1016/j.cherd.2018.09.003

Savvadelli, E., Kiouvrekis, Y., & Kokkinaki, A. (2026). A literature review on rule-based systems as decision support systems. *IFIP Advances in Information and Communication Technology, 761*, 376–388. https://doi.org/10.1007/978-3-032-02504-3_26

Segovia, P., Rajaoarisoa, L., Nejjari, F., Duviella, E., & Puig, V. (2019). A communication-based distributed model predictive control approach for large-scale systems.

Proceedings of the IEEE Conference on Decision and Control, 8366–8371. https://doi.org/10.1109/CDC40024.2019.9030085

Subbaraj, R., & Venkatraman, N. (2015). A systematic literature review on ontology based context management system. *Advances in Intelligent Systems and Computing, 338*, 609–619. https://doi.org/10.1007/978-3-319-13731-5_66

Tegicho, B. E., & Graves, C. (2021). Automatic emoji insertion based on environment context signals for the demonstration of pervasive computing features. *IEEE SoutheastCon Conference Proceedings*. https://doi.org/10.1109/SoutheastCon45413.2021.9401878

Vegega, C., Pytel, P., & Pollo-Cattaneo, M. F. (2019). Application of the requirements elicitation process for the construction of intelligent system-based predictive models in the education area. *Communications in Computer and Information Science, 1051*, 43–58. https://doi.org/10.1007/978-3-030-32475-9_4

Yamé, J. J., Gabsi, F., Darure, T., Jain, T., Hamelin, F., & Sauer, N. (2019). Optimality condition decomposition approach to distributed model predictive control. *Proceedings of the American Control Conference*, 742–747. https://doi.org/10.23919/ACC.2019.8814374