



Analisis Yuridis terhadap Kejahatan Finansial Modern: Perbandingan Pengaturan Hukum Pidana antara Crypto Crime dan Fintech Ilegal di Indonesia

A Legal Analysis of Modern Financial Crimes: A Comparison of Criminal Law Regulations between Crypto Crime and Illegal Fintech in Indonesia

Anisa¹, Zahra Destu Mulyani², Hudi Yusuf³

Fakultas Hukum, Universitas Bung Karno

Email: sukalumbaanisa@gmil.com¹, zahradestu77@gmail.com²

Article Info

Article history :

Received : 03-11-2025

Revised : 04-11-2025

Accepted : 06-11-2025

Published : 08-11-2025

Abstract

The fast development of digital technology has changed the global financial system, including in Indonesia. The rise of cryptocurrencies and fintech platforms has made financial services easier for people, but it has also brought new dangers like crypto-related crimes, digital investment scams, and illegal fintech businesses. This study looks at how Indonesia's criminal laws deal with these modern financial crimes in the digital age and examines who is responsible for these illegal activities and the platforms involved. The research uses a legal method that looks at laws, ideas, and real court cases. The results show that Indonesia's current laws, such as the Criminal Code, Law No. 11 of 2008 on Electronic Information and Transactions, and Law No. 8 of 2010 on Money Laundering, don't clearly cover digital assets. Because of this, law enforcement has trouble with rules, technical issues, and legal boundaries when dealing with crypto crimes. The study suggests creating new rules for digital asset-related crimes and improving teamwork between agencies to make criminal law enforcement more effective in the digital economy.

Keywords: *Criminal Law, Crypto Crime, Illegal Fintech*

Abstrak

Perkembangan teknologi digital telah mengubah cara masyarakat melakukan transaksi keuangan, termasuk di Indonesia. Munculnya aset kripto dan layanan fintech memberikan keuntungan bagi masyarakat, tetapi juga memicu berbagai masalah baru, seperti tindak pidana ekonomi modern seperti kejahatan kripto, penipuan investasi digital, dan keberadaan fintech ilegal. Penelitian ini bertujuan untuk menganalisis pengaturan hukum pidana di Indonesia terhadap kejahatan keuangan modern yang berbasis teknologi digital serta meninjau bentuk tanggung jawab hukum terhadap pelaku dan penyelenggara platform ilegal. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan peraturan perundang-undangan, konseptual, dan kasus. Hasil penelitian menunjukkan bahwa kerangka hukum nasional seperti KUHP, UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta UU Nomor 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang belum secara jelas mengatur kegiatan berbasis aset digital dan blockchain. Akibatnya, penerapan hukum terhadap kejahatan kripto dan fintech ilegal menghadapi kekurangan dalam segi norma, teknis, dan yurisdiksi lintas negara. Penelitian ini merekomendasikan adanya aturan khusus mengenai kejahatan keuangan berbasis aset digital serta peningkatan kerja sama antar lembaga untuk memperkuat penerapan hukum pidana di era ekonomi digital.

Kata Kunci: *Hukum Pidana, Kejahatan Kripto, Fintech Ilegal*



PENDAHULUAN

Perkembangan teknologi digital telah mengubah cara bertransaksi dan berinvestasi di sektor keuangan global, termasuk di Indonesia. Perubahan ini mendorong munculnya berbagai inovasi, seperti aset kripto dan layanan teknologi keuangan (fintech) yang memberikan kemudahan, efisiensi, serta akses yang lebih luas bagi masyarakat dalam melakukan berbagai jenis transaksi keuangan. Sekarang, ekosistem keuangan digital menjadi bagian yang sangat penting dalam perekonomian nasional, karena semakin banyak orang yang menggunakan internet dan aplikasi berbasis teknologi untuk melakukan pembayaran serta investasi secara daring.

Namun, kemajuan tersebut juga membawa tantangan baru berupa kejahatan finansial yang semakin rumit. Fenomena seperti kejahatan berbasis kripto, penipuan berdasarkan blockchain, serta praktik fintech gelap telah berkembang dengan cepat dan menyebabkan kerugian ekonomi yang besar. Sifat teknologi kripto yang tidak terpusat, anonim, dan lintas batas hukum membuat proses penegakan hukum menjadi lebih sulit, baik dalam mengidentifikasi pelaku maupun membuktikan tindak pidana. Kondisi ini memaksa hukum pidana perlu diperbarui agar dapat menyesuaikan diri dengan perkembangan teknologi keuangan.

Berbagai penelitian menunjukkan bahwa peraturan mengenai aset digital dan fintech di Indonesia belum lengkap dan hanya fokus pada sektor tertentu. Contohnya, regulasi mengenai aset kripto sekarang masih diberlakukan oleh Bappebti dan Bank Indonesia, yang lebih menekankan aspek ekonomi dan perlindungan pengguna, bukan aspek hukum pidana yang mengatur penindasan serta hukuman terhadap tindak kejahatan yang menggunakan aset digital. Selain itu, pengawasan terhadap fintech yang tidak sah sebagian besar dilakukan dengan cara administratif dan belum memiliki hukum pidana yang cukup kuat untuk mengganjar pelaku secara efektif.

Tidak adanya peraturan hukum pidana yang lengkap mengatur kejahatan berbasis kripto dan fintech ilegal menciptakan celah hukum yang bisa dimanfaatkan oleh pelaku tindak pidana. Selain itu, hal ini juga menyebabkan ketidakpastian hukum bagi para pelaku usaha, investor, serta masyarakat yang menggunakan layanan keuangan digital. Dalam pelaksanaan hukum, pihak yang bertugas menegakkan hukum sering mengalami hambatan dalam menentukan tempat kejadian perkara, membuktikan transaksi digital, serta menentukan pasal-pasal pidana yang tepat..

Oleh karena itu, penelitian ini diarahkan untuk menyelidiki dan memperbandingkan aturan hukum pidana terhadap tindak pidana kripto dan kegiatan fintech yang ilegal di Indonesia. Dengan melakukan analisis perbandingan, penelitian ini mencoba menyusun pendekatan hukum yang lebih fleksibel, menyeluruh, dan berhasil dalam menghadapi tantangan hukum pidana di masa kini yang semakin digital. Selain itu, penelitian ini juga diharapkan dapat memberikan saran untuk memperbarui sistem hukum pidana nasional agar sesuai dengan perkembangan teknologi keuangan global serta prinsip keadilan dalam dunia digital.

METODE PENELITIAN

Penelitian ini menerapkan pendekatan normatif hukum, yang merupakan cara riset hukum yang menitikberatkan pada analisis norma-norma hukum yang berlaku, prinsip-prinsip hukum, serta konsep-konsep hukum yang relevan dengan permasalahan yang dikaji. Pendekatan ini digunakan karena permasalahan dalam penelitian ini bersifat konseptual dan normatif, bukan empiris, yakni



terkait ketidaksinkronan dan kekosongan hukum pidana terhadap kejahatan finansial berbasis teknologi seperti *crypto crime* dan *fintech* ilegal di Indonesia.

Menurut Soerjono Soekanto (1996), penelitian hukum normatif bertujuan menemukan aturan, prinsip, dan doktrin hukum yang dapat digunakan untuk menjawab isu hukum tertentu. Penelitian ini berorientasi pada telaah bahan hukum yang ada untuk mengetahui konsistensi antara teori hukum dengan penerapan hukum positif. Sejalan dengan itu, Peter Mahmud Marzuki (2017) menegaskan bahwa penelitian hukum normatif lebih menitikberatkan pada proses analisis logis terhadap bahan hukum tertulis, seperti undang-undang, peraturan pemerintah, serta putusan pengadilan, bukan pada data empiris dari masyarakat (Widiarty, 2024).

Metode ini dianggap paling tepat karena penelitian ini berusaha menilai efektivitas kerangka hukum pidana nasional dalam menghadapi fenomena kejahatan finansial digital, serta merumuskan arah kebijakan hukum yang lebih adaptif di masa mendatang. Analisis dilakukan terhadap perangkat hukum yang telah ada — antara lain KUHP, UU ITE, dan UU TPPU — untuk melihat sejauh mana ketiganya mampu diterapkan terhadap bentuk-bentuk *cyber-financial crime* yang berkembang saat ini.

Sumber Data

Studi ini mengandalkan tiga kategori bahan hukum sebagai sumber data yang utama, yaitu:

1. Bahan Hukum Primer

Bahan hukum primer mencakup berbagai peraturan perundang-undangan yang memiliki kekuatan hukum langsung dan menjadi dasar utama dalam penelitian ini. Beberapa di antaranya meliputi Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahan dalam Undang-Undang Nomor 19 Tahun 2016, serta Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU). Selain itu, juga termasuk peraturan yang diterbitkan oleh Otoritas Jasa Keuangan (OJK) dan Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) yang mengatur mengenai aset digital, perlindungan konsumen di sektor keuangan, dan aktivitas finansial berbasis teknologi (fintech).

2. Bahan Hukum Sekunder

Bahan hukum sekunder mencakup berbagai sumber pendukung seperti literatur hukum, hasil penelitian ilmiah, artikel dalam jurnal akademik, laporan dari lembaga pemerintah, serta putusan pengadilan yang memiliki keterkaitan dengan topik penelitian. Sumber-sumber ini berperan penting dalam memperdalam pemahaman dan memperkuat analisis terhadap bahan hukum primer, khususnya dalam membangun kerangka teori hukum pidana yang relevan dengan perkembangan teknologi keuangan (fintech). Literatur yang digunakan dalam penelitian ini antara lain berasal dari karya Rahardjo (2006), Sabaruddin (2022), Simamora (2021), dan Nugraha (2020).

3. Bahan Hukum Tersier

Bahan hukum tersier meliputi berbagai sumber pendukung seperti kamus hukum, ensiklopedia hukum, serta referensi tambahan lainnya yang digunakan untuk membantu menjelaskan istilah-istilah hukum digital dan terminologi teknis dalam sektor keuangan modern. Sumber-sumber



ini berfungsi memperjelas makna konsep dan istilah yang digunakan dalam analisis hukum, sehingga pembahasan menjadi lebih akurat dan mudah dipahami.

Pendekatan Penelitian

Untuk mencapai hasil yang komprehensif, penelitian ini menggunakan tiga jenis pendekatan hukum utama, yaitu:

1. Pendekatan Perundang-undangan (Statute Approach)

Pendekatan ini dilakukan dengan menelaah dan menafsirkan seluruh peraturan perundang-undangan yang berkaitan dengan aset kripto, *fintech*, dan hukum pidana nasional. Tujuannya untuk menemukan sinkronisasi vertikal dan horizontal antaraturan hukum yang berlaku serta mengidentifikasi potensi kekosongan hukum yang perlu diperbarui agar sesuai dengan perkembangan digital.

2. Pendekatan Konseptual (Conceptual Approach)

Pendekatan ini menitik beratkan dalam kajian dasar-dasar dan prinsip-prinsip hukum yang menjadi landasan peraturan yang bersangkutan, seperti asas legalitas, asas pertanggungjawaban pidana, dan asas netralitas teknologi (technological neutrality). Pendekatan ini penting untuk memahami bagaimana teori hukum dapat diterapkan dalam konteks kejahatan siber yang terus berkembang (Rahardjo, 2006; Sabaruddin, 2022).

3. Pendekatan Kasus (Case Approach)

Metode ini diimplementasikan melalui analisis berbagai contoh nyata yang terkait dengan kejahatan *crypto crime* dan *fintech* ilegal di Indonesia maupun di negara lain. Misalnya, kasus penipuan investasi aset digital yang ditangani oleh Bareskrim Polri dan kasus pelanggaran sistem pembayaran daring oleh penyelenggara *fintech* tanpa izin. Pendekatan ini digunakan untuk memahami bagaimana norma hukum diterapkan secara praktis, sekaligus mengidentifikasi kelemahan dalam sistem penegakan hukum (Simamora, 2021; Nugraha 2020).

Kesimpulan Metodologis

Dengan menggabungkan ketiga pendekatan tersebut, penelitian ini berupaya memberikan analisis komprehensif dan preskriptif terhadap efektivitas pengaturan hukum pidana di Indonesia dalam menghadapi tantangan kejahatan finansial digital. Hasil analisis diharapkan mampu merumuskan rekomendasi pembaruan hukum yang selaras dengan perkembangan teknologi finansial dan prinsip keadilan hukum modern.

HASIL DAN PEMBAHASAN

1. Konseptualisasi Kejahatan Finansial Digital

Kejahatan finansial digital merupakan fenomena hukum yang lahir dari transformasi teknologi informasi dan digitalisasi sistem keuangan global. Perkembangan teknologi *blockchain*, *artificial intelligence* (AI), dan sistem pembayaran digital telah menciptakan ekosistem keuangan baru yang cepat, efisien, dan terdesentralisasi. Namun, di sisi lain, kemajuan ini juga memperluas ruang kejahatan dengan munculnya berbagai bentuk *cyber-*



financial crime yang sulit dijangkau oleh instrumen hukum konvensional (Maras, 2016). Secara umum, kejahatan finansial digital dapat didefinisikan sebagai segala bentuk tindakan melawan hukum yang menggunakan sistem elektronik atau teknologi digital untuk memperoleh keuntungan ekonomi secara tidak sah (UNODC, 2021). Dalam konteks ini, dua bentuk kejahatan menonjol di Indonesia adalah **crypto crime** dan **fintech ilegal** — keduanya menunjukkan tantangan serius terhadap sistem hukum pidana nasional yang masih berbasis regulasi tradisional.

a. Crypto Crime

Secara konseptual, crypto crime merupakan tindak pidana yang menggunakan atau menjadikan aset kripto (cryptocurrency) sebagai sarana, objek, maupun hasil kejahatan. Maras (2016) mendefinisikan *crypto-related crime* sebagai kejahatan yang memanfaatkan infrastruktur teknologi *blockchain* untuk melakukan tindakan ilegal, seperti penipuan investasi digital, *ransomware*, pencurian data, atau pencucian uang lintas batas (Houben et al, 2018).

Dalam konteks hukum pidana, kejahatan kripto sering dikategorikan ke dalam tiga bentuk utama:

- 1) **Kejahatan dengan kripto sebagai alat (means)** – misalnya pembayaran tindak pidana melalui Bitcoin atau aset kripto lain.
- 2) **Kejahatan dengan kripto sebagai objek (object)** – seperti pencurian atau peretasan dompet digital (*wallet phishing*).
- 3) **Kejahatan dengan kripto sebagai hasil (proceeds)** – yakni tindak pidana yang menggunakan konversi kripto untuk menyamarkan asal-usul uang (*money laundering*).

Karakteristik utama crypto crime adalah **anonimitas, desentralisasi, dan globalitas transaksi**, yang menyebabkan kesulitan pembuktian serta pelacakan pelaku (Ying, 2022). Bahkan, dalam laporan **Europol (2023)** disebutkan bahwa lebih dari 60% kasus pencucian uang lintas negara pada 2022 melibatkan aset digital. Oleh karena itu, regulasi Hukum pidana yang berbasis teritorial mulai kehilangan relevansinya untuk menangani tindakan kriminal yang bersifat lintas batas (*transnational crime*).

b. Fintech Ilegal

Sementara itu, **fintech ilegal** mengacu pada penyelenggaraan layanan keuangan digital yang beroperasi tanpa izin dari Otoritas Jasa Keuangan (OJK) ataupun Bank Indonesia. Layanan ini meliputi kegiatan peminjaman antar individu (P2P), penggalangan dana, pembayaran digital, sampai perdagangan aset kripto yang dilakukan melalui aplikasi tanpa izin (Simamora, 2021). Kehadiran fintech yang tidak sah tidak hanya berakibat pada kerugian finansial bagi masyarakat, tapi juga menghadirkan **risiko hukum dan sosial**, seperti:

- 1) Penyalahgunaan data pribadi nasabah tanpa persetujuan,
- 2) Pemerasan digital melalui penagihan yang bersifat intimidatif,



- 3) Praktik bunga tinggi (predatory lending) yang melanggar prinsip keadilan kontraktual,
- 4) Transaksi lintas negara tanpa perlindungan hukum domestik.

Menurut data OJK (2023) (Herawati, 2024), sejak tahun 2018 hingga 2023, lebih dari 5.000 platform fintech ilegal telah diblokir di Indonesia karena pelanggaran izin dan praktik keuangan yang merugikan konsumen. Kondisi ini menggambarkan lemahnya sistem pengawasan hukum nasional terhadap sektor keuangan berbasis teknologi.

c. Perspektif Adaptasi Hukum

Dalam pandangan **Rahardjo (2006)**, hukum tidak boleh statis, melainkan harus bersifat **adaptif terhadap perubahan sosial dan teknologi**. Perubahan struktur ekonomi digital menuntut sistem hukum pidana untuk melakukan **penyesuaian paradigma**, dari *repressive law enforcement* menjadi *preventive and adaptive regulation*. Artinya, hukum tidak hanya berfungsi menindak, tetapi juga mengantisipasi risiko kejahatan finansial yang berbasis inovasi teknologi (Rahardjo, 2006).

Dengan demikian, konseptualisasi kejahatan finansial digital menegaskan perlunya **reformulasi kebijakan hukum pidana nasional** yang mampu menyeimbangkan antara **inovasi teknologi keuangan** dan **perlindungan hukum bagi masyarakat**. Indonesia membutuhkan perangkat hukum yang bersifat **teknologi-netral (technological neutrality)**, agar penegakan hukum tetap relevan terhadap perkembangan kripto dan fintech global tanpa menghambat kemajuan ekonomi digital.

2. Karakteristik dan Modus Crypto Crime di Indonesia

Perkembangan aset kripto di Indonesia menunjukkan tren yang semakin meningkat sejak **Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti)** telah memberikan pengakuan resmi terhadap aset kripto sebagai komoditas yang sah untuk diperdagangkan melalui Peraturan Bappebti Nomor 5 Tahun 2019 (Barkah, 2023). Pengakuan ini mendorong tumbuhnya ekosistem perdagangan aset digital, tetapi di sisi lain juga melahirkan berbagai bentuk penyalahgunaan kripto untuk kejahatan finansial. Regulasi yang masih terbatas pada aspek perdagangan (*trading regulation*) tanpa pengaturan khusus mengenai aspek pidana, membuka ruang terjadinya praktik kejahatan berbasis aset digital.

Menurut **Arner, Barberis, dan Buckley (2017)**, kemunculan *crypto-assets* menciptakan bentuk risiko hukum baru yang belum terakomodasi oleh sistem keuangan tradisional, terutama karena karakteristik desentralisasi, anonimitas, dan ketiadaan otoritas pengatur tunggal. Di Indonesia, kondisi tersebut tampak dari maraknya berbagai **modus crypto crime** yang kerap terjadi dalam bentuk:

a. Skema Ponzi berbasis token digital.

Modus ini dilakukan dengan menjanjikan keuntungan tinggi melalui penjualan token baru (*initial coin offering* palsu) atau aset kripto tanpa nilai riil. Kasus seperti **investasi bodong E-Dinar Coin dan Viral Blast Global** merupakan contoh praktik *crypto Ponzi scheme* yang mengelabui masyarakat dengan iming-iming keuntungan cepat (Saputra, 2022; Wiryawan, 2023).

b. Phishing wallet dan pencurian data pengguna.



Dalam modus ini, pelaku memperoleh akses ke **private key** dompet digital korban melalui situs palsu atau tautan berbahaya. Studi **Kethineni, Cao, dan Dodge (2018)** menunjukkan bahwa praktik *wallet phishing* dan *exchange hacking* merupakan pola umum kejahatan kripto global yang juga ditemukan di Asia Tenggara, termasuk Indonesia.

c. **Pencucian uang (money laundering) melalui aset digital.**

Pelaku kejahatan memanfaatkan konversi aset kripto lintas negara untuk menyamarkan asal-usul dana hasil tindak pidana. **Houben & Snyers (2018)** menegaskan bahwa kripto sering digunakan sebagai media *layering* dalam proses pencucian uang karena sulit dilacak oleh otoritas keuangan tradisional.

Kasus **binary option** yang melibatkan figur publik seperti **Indra Kenz dan Donny Salmanan** menjadi contoh nyata lemahnya sistem hukum nasional dalam mengklasifikasikan dan menindak kejahatan berbasis aset digital. Meski secara hukum tidak termasuk aset kripto murni, pola investasi dan mekanisme perdagangannya memiliki kesamaan dengan *crypto-based trading fraud* yang dikategorikan sebagai penipuan investasi digital (Kominfo, 2022; Hanoatubun, 2023).

Menurut laporan resmi Bappebti (2023), terdapat lebih dari 150 entitas perdagangan aset kripto tidak berizin yang beroperasi di Indonesia, sebagian besar berbasis di luar negeri. Kondisi ini menimbulkan tantangan serius bagi penegakan hukum karena menyangkut yurisdiksi lintas batas (cross-border jurisdiction). Oleh karena itu, dibutuhkan suatu pendekatan hukum yang bersifat adaptif, dan kolaboratif antara Bappebti, Otoritas Jasa Keuangan (OJK), dan Kepolisian RI, agar pengawasan dan penindakan terhadap tindak pidana kripto dapat dilakukan secara terpadu dan lintas sektor.

Pendekatan semacam ini juga sejalan dengan pandangan **Rahardjo (2006)** bahwa sistem hukum harus bersifat responsif dan antisipatif terhadap perubahan sosial, termasuk terhadap perkembangan ekonomi digital. Dengan demikian, strategi penegakan hukum terhadap *crypto crime* di Indonesia perlu diarahkan pada model yang technologically neutral namun efektif dalam menjerat pelaku kejahatan lintas batas.

3. Dinamika Hukum terhadap Fintech Ilegal di Indonesia

Fintech ilegal adalah salah satu jenis kejahatan finansial digital yang sering menyebabkan kerugian besar bagi masyarakat dan perekonomian di Indonesia. Menurut laporan Satgas Waspada Investasi (OJK, 2023), sejak tahun 2018 hingga 2023, sudah tercatat lebih dari 5.000 lembaga fintech pembiayaan ilegal yang ditutup karena beroperasi tanpa izin, mengakses data pribadi tanpa izin, serta melakukan penagihan yang melanggar hukum dan norma sosial. Hal ini menunjukkan bahwa masyarakat masih kurang memahami hukum digital dan belum siap secara hukum menghadapi perkembangan teknologi keuangan (Budiman & SH, 2025).

Karakteristik umum fintech ilegal di Indonesia adalah sebagai berikut:

- Belum memperoleh lisensi resmi dari Otoritas Jasa Keuangan (OJK) ataupun Bank Indonesia, Mengumpulkan dan mengakses data pribadi pengguna tanpa izin yang sah,



- b. Mengenakan bunga yang terlalu tinggi dan menerapkan sistem penagihan yang menakutkan,
- c. Tidak memberi informasi jelas mengenai biaya, risiko, dan cara kerja perjanjian pinjaman.

Secara hukum, pelaku fintech ilegal bisa dikenai pasal 30 dan 32 Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (UU ITE), yang mengatur masalah akses tidak sah dan perubahan data elektronik, serta pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) mengenai penipuan. Walaupun begitu, pelaksanaan ketentuan-ketentuan tersebut masih terbatas, karena bukti digital seringkali bersifat lintas batas dan sulit dibuktikan di pengadilan

Dalam penerapan di lapangan, penegakan hukum terhadap fintech ilegal masih menghadapi beberapa tantangan, antara lain:

- a. Kurangnya kemampuan dalam membuktikan peristiwa forensik digital,
- b. Minimnya keselarasan kerja antara OJK, Kepolisian, dan Kementerian Komunikasi dan Informatika,
- c. Tidak adanya undang-undang khusus mengenai fintech dan aset digital yang mengatur batas pidana serta kewenangan pengawasan lintas sektor.

Menurut Simamora (2021), penegakan hukum terhadap fintech ilegal di Indonesia masih bersifat reaktif dan tidak menyeluruh, hanya memperhatikan kasus setelah terjadi kerugian, tanpa tindakan pencegahan berdasarkan pemahaman hukum dan pengawasan terus menerus.

Oleh karena itu, dibutuhkan perbaikan hukum dengan pendekatan "policy-oriented law", yang menggabungkan aturan keuangan, perlindungan data pribadi, serta penerapan hukum pidana digital secara terpadu.

Beberapa negara, seperti Singapura dan Inggris, telah menerapkan sistem pengawasan yang berbasis risiko, dengan mengatur fintech dan aset digital di bawah otoritas tunggal seperti Monetary Authority of Singapore (MAS) dan Financial Conduct Authority (FCA). Model ini berhasil dalam mengimbangi inovasi teknologi dengan perlindungan hukum bagi konsumen. Indonesia bisa mengadopsi pendekatan serupa dengan memperkuat kemampuan lembaga seperti Bappebti dan OJK, serta memperluas kewenangan penyelidikan terhadap kejahatan finansial digital lintas batas (Sabaruddin, 2022).

4. Ketidaksesuaian (Gap) Hukum Positif terhadap Kejahatan Digital

Ketidaksesuaian antara hukum positif dan kejahatan digital di Indonesia terlihat dari belum adanya aturan pidana yang secara jelas mengatur aktivitas berbasis teknologi kripto dan fintech. Rephrase Not Available meskipun KUHP, UU ITE, dan UU TPPU sudah menjadi dasar hukum untuk menangani kejahatan siber, norma-norma dalam peraturan tersebut belum bisa menjangkau jenis kejahatan baru yang memanfaatkan teknologi blockchain dan aset digital. Menurut Prakoso & Siregar (2021), kekosongan hukum ini terjadi karena pendekatan hukum yang masih "berorientasi pada objek fisik," sementara kejahatan finansial digital berjalan dalam sistem desentralisasi yang tidak memiliki batas hukum. Hal ini menyebabkan kesulitan dalam menentukan tempat kejahatan terjadi dan siapa pelakunya, terutama ketika transaksi



dilakukan melalui platform di luar negeri. Selain itu, menurut Wulandari (2022), hukum positif Indonesia masih bersifat represif dan belum mampu menyesuaikan diri dengan perkembangan dunia digital. Regulasi baru seperti Rancangan Undang-Undang Perlindungan Data Pribadi dan revisi UU ITE belum sepenuhnya mengatur tanggung jawab pidana dalam aktivitas kejahatan kripto dan fintech ilegal. Kesenjangan ini menciptakan celah normatif antara perkembangan teknologi keuangan dengan kemampuan sistem hukum nasional, sehingga diperlukan pembaruan hukum yang menerapkan pendekatan neutrality teknologi dan regulasi berbasis risiko. Selain itu, Sabaruddin (2022) mengatakan bahwa peraturan hukum pidana di Indonesia belum memperhatikan prinsip teknologi netral, yaitu prinsip bahwa aturan hukum harus tetap relevan meskipun teknologi terus berkembang. Prinsip ini sudah diterapkan di Uni Eropa lewat Regulasi Perlindungan Data Umum (GDPR) dan dalam Undang-Undang Keamanan Online Inggris (2023), yang memastikan aturan hukum bisa fleksibel mengikuti inovasi teknologi digital. Dari sudut pandang kelembagaan, ada ketidaksesuaian karena adanya tumpang tindih wewenang antara OJK, Bappebti, BI, dan PPATK. Setiap lembaga mengatur sektor yang berbeda, tetapi tidak ada integrasi hukum yang kuat. Menurut Budiman & S.H. (2025), penerapan hukum terhadap kejahatan finansial digital membutuhkan sistem koordinasi lintas lembaga yang didasarkan pada pemerintahan berbasis data.

5. Komparasi Yuridis: Crypto Crime vs Fintech Ilegal

Dari sudut hukum, kejahatan crypto dan fintech ilegal memiliki kesamaan dalam penggunaan teknologi digital untuk memperoleh keuntungan secara tidak sah. Namun keduanya berbeda dalam hal objek yang diperlakukan, jenis pelanggaran, serta sistem pengawasan yang berlaku. Kejahatan crypto berkaitan dengan penggunaan aset digital seperti cryptocurrency sebagai alat atau hasil dari tindak pidana lintas batas. Sementara fintech ilegal melibatkan penyelenggaraan layanan keuangan tanpa memiliki izin resmi, biasanya dalam skala lokal. Menurut Suryani (2023), kejahatan crypto umumnya diatur dalam UU ITE, UU TPPU, serta peraturan Bappebti. Sementara itu, fintech ilegal diatur oleh UU Perlindungan Konsumen dan peraturan OJK. Meski berbeda, kedua jenis kejahatan tersebut menghadapi tantangan yang sama dalam proses pembuktian digital dan kerja sama antar instansi (Suryani, 2023).

6. Tanggung Jawab Pidana dan Aspek Pembuktian

Pertanggungjawaban hukum dalam kasus kejahatan finansial berbasis digital memiliki dua sisi, yaitu bisa dikenakan kepada individu maupun perusahaan yang mengelola platform tersebut. Menurut Nasution (2021), konsep tanggung jawab pidana perusahaan harus diterapkan dalam kasus kejahatan fintech, karena banyak pelanggaran dilakukan secara terencana oleh badan hukum berbentuk perusahaan. Dalam kasus kejahatan kripto, tanggung jawab hukum juga bisa dikenakan kepada pihak yang membantu aktivitas ilegal, misalnya penyedia bursa kripto yang tidak memiliki izin. Namun, dalam memproses kasus ini membutuhkan metode pembuktian yang baru. Menurut Rahmawati (2023), penggunaan digital forensik dan alat pelacakan blockchain seperti Chainalysis sangat penting untuk menelusuri arus transaksi kripto (Nasution, 2021).

Masalah utama dalam proses pembuktian adalah sifat anonim dan terenkripsi dari blockchain, sehingga penyidik sering kali harus bekerja sama dengan negara lain melalui



Mutual Legal Assistance (MLA). Di sisi lain, proses hukum masih mengalami hambatan karena belum semua jenis bukti digital diakui secara resmi dalam pengadilan. Karena itu, sistem hukum Indonesia perlu memperkuat mekanisme pembuktian digital dengan memperbarui Peraturan (KUHAP) dan Undang-Undang ITE agar bukti berupa catatan digital diakui secara setara dengan bukti biasa.

7. Reformulasi Kebijakan Hukum Pidana

Menghadapi tantangan yang kompleks dalam kejahatan finansial digital, kebijakan hukum pidana nasional perlu diubah berdasarkan prinsip reformasi hukum yang berfokus pada kebijakan. Perubahan ini harus mencakup aspek berupa isi, bentuk, dan budaya hukum (Lawrence M. Friedman, 1975).

- a. Isi hukum: Pembuatan Rancangan Undang-Undang tentang Kejahatan Keuangan Digital sangat penting agar bisa menangani jenis tindak pidana baru seperti penipuan kripto, pencucian dana digital, dan penipuan fintech. Budiman & S.H. (2025) menekankan perlunya regulasi yang netral secara teknologi agar tetap seimbang antara inovasi dan perlindungan masyarakat.
- b. Bentuk hukum: Diperlukan kemitraan antar institusi seperti OJK, PPATK, Bappebti, Polri, dan Kominfo melalui pembentukan Task Force Nasional Terkait Kejahatan Finansial Digital. Hal ini sesuai dengan praktik Financial Conduct Authority (FCA) Inggris dan Monetary Authority of Singapore (MAS) yang menerapkan regulasi berdasarkan risiko.
- c. Budaya hukum: Hanoatubun (2024) menekankan pentingnya meningkatkan kemampuan aparatur hukum dan kesadaran masyarakat tentang dunia digital agar mencegah terjadinya kejahatan finansial. Edukasi masyarakat tentang keamanan dalam transaksi dan penegakan hukum yang berbasis teknologi perlu menjadi bagian dari rencana nasional.

Dengan melakukan reformasi secara menyeluruh, sistem hukum pidana Indonesia bisa berubah dari sistem yang hanya merespons kejadian sesudah terjadi menjadi sistem yang mencegah dan bekerja sama antar lembaga, sesuai arah kebijakan hukum modern.

KESIMPULAN

Perkembangan teknologi digital membawa kemudahan dalam sektor keuangan melalui aset kripto dan layanan fintech, namun pada saat yang sama juga menghadirkan tantangan baru berupa kejahatan finansial modern. Indonesia masih mengalami kesenjangan (gap) antara perkembangan teknologi dan kemampuan hukum positif dalam mengatur serta menindak kejahatan tersebut. Hal ini disebabkan karena ketentuan dalam KUHP, UU ITE, dan UU TPPU belum secara jelas mengatur aset digital, blockchain, maupun operasional fintech yang ilegal. Crypto crime memiliki karakter lintas negara, anonim, dan desentralistik sehingga menyulitkan penegakan hukum baik dari segi pembuktian maupun yurisdiksi. Sementara fintech ilegal lebih bersifat lokal, namun menimbulkan dampak besar seperti penyalahgunaan data pribadi, penipuan digital, hingga praktik bunga pinjaman tidak wajar. Kedua fenomena tersebut sama-sama menunjukkan lemahnya perlindungan hukum dan koordinasi antar lembaga seperti OJK, Bappebti, BI, Kominfo, dan Kepolisian.



Melalui analisis komparatif, dapat disimpulkan bahwa sistem hukum pidana Indonesia masih bersifat represif dan reaktif, bukan preventif dan adaptif terhadap kejahatan finansial digital. Penegakan hukum juga menghadapi hambatan berupa belum diakuinya bukti digital secara optimal, kurangnya perangkat forensik siber, serta keterbatasan kerja sama internasional. Oleh karena itu, diperlukan reformulasi kebijakan hukum pidana yang meliputi:

1. Pembentukan undang-undang khusus tentang kejahatan keuangan digital,
2. Penguatan koordinasi antar lembaga melalui task force nasional, dan
3. Peningkatan literasi digital serta kapasitas aparat penegak hukum.

Dengan langkah tersebut, sistem hukum pidana Indonesia diharapkan mampu berubah dari sistem yang hanya menanggapi kejahatan setelah terjadi menjadi sistem yang mampu mencegah, mendeteksi, dan menindak secara efektif kejahatan finansial modern dalam ekosistem ekonomi digital.

DAFTAR PUSTAKA

- Barkah, L. B., & Zakiran, A. H. (2023). Perlindungan Hukum Terhadap Investor Aset Digital Kripto Ditinjau dari Peraturan Bappebti Nomor 5 Tahun 2019 Tentang Ketentuan Teknis Penyelenggaraan Pasar
- Budiman, R., & S.H., D. (2025). Kebijakan Hukum Pidana terhadap Fintech dan Aset Digital di Indonesia. *Jurnal Rechtsvinding*, 14(2), 301-322.
- Budiman, R., & S.H., D. (2025). Kebijakan Hukum Pidana terhadap Fintech dan Aset Digital di Indonesia. *Jurnal Rechtsvinding*, 14(2), 301–322.
- Hanoatubun, S. (2024). Reformulasi Kebijakan Hukum Pidana di Era Digitalisasi Ekonomi. *Jurnal Ilmu Hukum*, 5(1), 11–29
- Nasution, A. (2021). Pertanggungjawaban Pidana dalam Tindak Pidana Siber Berbasis Aset Kripto. *Jurnal Hukum IUS QUA IUSTUM*, 28(2), 233–250.
- Prakoso, R., & Siregar, R. (2021). Analisis Kekosongan Norma Hukum terhadap Kejahatan Digital di Indonesia. *Jurnal Rechtsvinding*, 10(2), 201–223.
- Rahmawati, D. (2023). Pembuktian Digital dalam Kasus Kejahatan Siber: Tantangan dan Solusi Hukum di Indonesia. *Jurnal Hukum Lex Renaissance*, 8(1), 45–61.
- Saputra, R. Analisis Hukum terhadap Penipuan Berbasis Kripto di Indonesia. *Jurnal Rechtsvinding*, 11(2), 133–150.
- Simamora, F. (2021). “Penegakan Hukum terhadap Fintech Ilegal di Indonesia 18(2), 245–260
- Suryani, D. (2023). Komparasi Pengaturan Hukum terhadap Kejahatan Fintech dan Kripto di Indonesia. *Jurnal Lex Renaissance*, 8(2), 141–162.