SAMUDRA SOLUSI PROFESIONAL

MENGUNGKAP RAHASIA CRYPTOCURRENCY

Perspektif Hukum Pidana Islam

dalam Menanggulangi Kejahatan Ekonomi Digital

Dr. R. Arif Muljohadi, S.H., M.Hum.

MENGUNGKAP RAHASIA
CRYPTOCURRENCY

Perspektif Hukum Pidana Islam dalam Menanggulangi Kejahatan Ekonomi Digital

Dr. R. Arif Muljohadi, S.H., M.Hum.

MENGUNGKAP RAHASIA
CRYPTOCURRENCY

Perspektif Hukum Pidana Islam dalam Menanggulangi Kejahatan Ekonomi Digital

Diterbitkan Oleh:

SAMUDRA SOLUSI PROFESIONAL

PT. Samudra Solusi Profesional

Perpustakaan Nasional RI : Katalog Dalam Terbitan (KDT)

JUDUL DAN PENANGGUNG JAWAB	Mengungkap Rahasia Cryptocurrency : Perspektif Hukum Pidana Islam dalam Menanggulangi Kejahatan Ekonomi Digital / Dr. R. Arif Muljohadi, S.H., M.Hum. / editor, Abdul Gafur Rinaldi, S.Ak., M.Sc., CTT., BKP.
EDISI	Cetakan Pertama, November 2025
PUBLIKASI	Malang : PT Samudra Solusi Profesional, 2025
DESKRIPSI FISIK	306 halaman ; 23 cm
IDENTIFIKASI	ISBN : 978-634-7296-94-8
SUBJEK	Cessie dalam Aras Ius Aequum Perikatan

MENGUNGKAP RAHASIA CRYPTOCURRENCY: PERSPEKTIF HUKUM PIDANA ISLAM DALAM MENANGGULANGI KEJAHATAN EKONOMI DIGITAL

Penulis: Dr. R. Arif Muljohadi, S.H., M.Hum.

Editor: Abdul Gafur Rinaldi, S.Ak., M.Sc., CTT. BKP.
Layouter: Shanty Dwi Rachmawati
Desain Cover: La_Chus99
Diterbitkan Oleh:

SAMUDRA SOLUSI PROFESIONAL

Anggota IKAPI
No. Registrasi Keanggotaan: 385/JTI/2023

Kantor Pusat
Bukit Cemara Tidar Blok K1 No. 14
Desa/Kelurahan Karangbesuki, Kec. Sukun,
Kota Malang, Jawa Timur
Telp/Fax: 0822-3118-6542
Email: samudrasolusiprofesional@gmail.com

Kantor Cabang
- Workshop Jasmine, Jasmine Valley Blok 3 No. 2, Araya, Malang
- Jalan Magelang, No. 118 Karangwaru, Tegalrejo, D.I Yogyakarta

Cetakan Pertama, November 2025
ISBN: 978-634-7296-94-8

Kata Pengantar

Bismillāhirraḥmānirraḥīm,

Segala puji bagi Allah SWT, Tuhan semesta alam, yang dengan rahmat dan karunia-Nya telah memungkinkan terwujudnya karya sederhana ini. Shalawat serta salam semoga senantiasa tercurah kepada junjungan kita, Nabi Muhammad SAW, sang pembawa risalah pencerahan yang menjadi teladan utama dalam menegakkan keadilan dan kemaslahatan.

Kita hidup di sebuah zaman yang ditandai oleh disrupsi. Gelombang inovasi teknologi, khususnya dalam satu dekade terakhir, telah mengubah lanskap ekonomi, sosial, dan bahkan cara kita berinteraksi secara fundamental. Di jantung perubahan ini, denyut teknologi *blockchain* dan *cryptocurrency* berdetak paling kencang, menjanjikan sebuah era baru keuangan yang lebih terdesentralisasi, transparan, dan inklusif. Namun, seperti dua sisi mata uang, di balik kilau potensi inovasi tersebut, tersembunyi bayang-bayang risiko yang tak kalah besar.

Buku ini lahir dari sebuah kegelisahan intelektual. Kegelisahan melihat bagaimana teknologi yang sama, yang digadang-gadang sebagai pembebas, justru dieksploitasi menjadi sarana kejahatan ekonomi yang memakan korban ribuan orang di negeri ini. Penipuan berkedok investasi, skema pencucian uang yang semakin licin, hingga pendanaan aktivitas terorisme, semuanya menemukan medium baru yang subur di dunia *cryptocurrency*. Fenomena ini memaksa kita untuk berhenti sejenak dan merenung: Sudah siapkah kerangka hukum kita—baik hukum positif maupun hukum Islam—menghadapi tantangan zaman ini?

Pertanyaan inilah yang menjadi kompas dalam penulisan buku ini. Kami berupaya untuk tidak sekadar menyajikan paparan teknis tentang *cryptocurrency*, tetapi juga melakukan sebuah perjalanan intelektual yang melintasi batas-batas disiplin ilmu. Kami menyelami kedalaman samudra fikih jinayah untuk menemukan mutiara-mutiara prinsip yang ternyata masih sangat relevan, lalu membandingkannya dengan perangkat hukum positif yang kita miliki. Tujuannya adalah untuk membuktikan bahwa tradisi intelektual Islam, melalui konsep *jarimah ta'zir* dan *Maqashid al-Shari'ah*, bukanlah sesuatu yang statis dan usang, melainkan sebuah sistem yang dinamis dan memiliki kapasitas luar biasa untuk beradaptasi dan memberikan solusi.

Karya ini disusun bukan untuk memberikan jawaban akhir yang absolut. Sebaliknya, ia dimaksudkan sebagai sebuah pembuka dialog—sebuah pemantik diskusi antara para legislator, aparat penegak hukum, praktisi industri, akademisi, para ulama, dan masyarakat luas. Kami percaya bahwa tantangan sekompleks ini tidak dapat diatasi secara parsial. Diperlukan sebuah "ijtihad kolektif" era modern, sebuah sinergi holistik di mana setiap elemen bangsa mengambil perannya masing-masing.

Kepada para pembaca, kami berharap buku ini tidak hanya menjadi sumber informasi, tetapi juga sumber inspirasi. Inspirasi untuk lebih waspada, lebih kritis, dan lebih peduli. Inspirasi bagi para mahasiswa untuk menekuni kajian interdisipliner yang relevan dengan zaman. Inspirasi bagi para regulator untuk merumuskan kebijakan yang bijak. Dan inspirasi bagi para inovator untuk menciptakan teknologi yang tidak hanya mengejar keuntungan, tetapi juga menjunjung tinggi etika dan keadilan.

Tentu, karya ini jauh dari kesempurnaan. Segala kekurangan dan kekhilafan yang ada di dalamnya sepenuhnya menjadi tanggung jawab kami sebagai penulis. Kami sangat terbuka terhadap segala bentuk kritik dan masukan yang membangun demi penyempurnaan di masa mendatang.

Akhir kata, kami mengucapkan terima kasih yang tulus kepada semua pihak yang telah memberikan dukungan, baik moril maupun materiel, selama proses penulisan buku ini. Semoga karya sederhana ini dapat menjadi sebutir pasir di tengah gurun ilmu pengetahuan dan memberikan

manfaat, walau sekecil apa pun, bagi upaya kita bersama dalam membangun ekosistem ekonomi digital Indonesia yang aman, adil, dan membawa kemaslahatan bagi seluruh umat manusia.

Wallāhu a'lam biṣ-ṣawāb.

Yogyakarta, November 2025

Dr. R. Arif Muljohadi, S.H., M.Hum.

Daftar Isi

BAB 3

BAB 4

BAB 5

BAB 6

BAB 7

BAB 8

BAB 12

BAB 13

BAB 14

BAB 1

Prolog: Cryptocurrency dan Ekonomi Digital

Dalam konstelasi keilmuan kontemporer, diskursus mengenai ekonomi digital dan *cryptocurrency* telah menjadi arena perdebatan yang dinamis, melibatkan pakar ekonomi, teknologi, hukum, dan teologi. Kemunculan aset kripto bukan sekadar inovasi teknologi, melainkan sebuah fenomena sosio-ekonomi yang secara fundamental menantang hegemoni sistem keuangan berbasis fiat yang selama ini didominasi oleh otoritas moneter sentral (Nakamoto, 2008). Bab ini memposisikan diri sebagai jembatan antara pemahaman teknis mengenai *cryptocurrency* dan analisis yuridis-filosofis terhadap implikasinya. *Research gap* (celah penelitian) yang hendak diisi adalah kurangnya analisis sistematis yang mengintegrasikan pemahaman evolusi sistem keuangan, definisi teknis aset kripto, konteks ekonomi digital Indonesia, dan urgensi penegakan hukum pidana Islam dalam satu kerangka pembahasan yang koheren. Dengan demikian, pertanyaan penelitian utama yang akan dijawab oleh bab ini adalah: Bagaimana evolusi sistem keuangan melahirkan *cryptocurrency*, dan mengapa kompleksitas kejahatan yang menyertainya dalam ekonomi digital Indonesia memerlukan analisis mendalam dari perspektif hukum pidana Islam?

A. Evolusi Uang dan Sistem Keuangan

Sub-bab ini melakukan penelusuran historis dan konseptual terhadap evolusi sistem moneter, dari bentuknya yang paling primitif hingga arsitektur keuangan modern. Tujuannya adalah untuk memberikan konteks mengapa inovasi radikal seperti *cryptocurrency* dan Keuangan Terdesentralisasi (DeFi) dapat muncul sebagai respons terhadap keterbatasan dan krisis yang melekat pada sistem sebelumnya. Analisis dimulai dari transisi sistem barter ke uang komoditas dan fiat, dilanjutkan dengan pembahasan peran institusi sentral dalam menjaga stabilitas moneter, hingga dampak krisis keuangan global sebagai katalisator utama bagi pencarian alternatif sistem keuangan.

1. Sejarah Sistem Barter hingga Uang Fiat

Evolusi uang merupakan cerminan dari evolusi peradaban manusia dalam mencari medium pertukaran yang efisien. Pada mulanya, masyarakat agraris bergantung pada sistem barter, yaitu pertukaran langsung barang dengan barang. Namun, sistem ini memiliki kelemahan fundamental yang dikenal sebagai *double coincidence of wants* (kesamaan keinginan

ganda), di mana transaksi hanya dapat terjadi jika kedua belah pihak saling menginginkan barang yang dimiliki oleh pihak lain (Mankiw, 2021). Keterbatasan ini mendorong lahirnya uang komoditas, seperti garam, kerang, atau logam mulia, yang memiliki nilai intrinsik dan diterima secara umum sebagai medium pertukaran.

Perkembangan selanjutnya adalah penggunaan logam mulia, terutama emas dan perak, yang memiliki karakteristik ideal sebagai uang: tahan lama, mudah dibawa, dapat dibagi (*divisible*), dan nilainya relatif stabil. Era ini kemudian melahirkan uang representatif, di mana sertifikat kertas atau koin diterbitkan oleh otoritas terpercaya sebagai klaim atas sejumlah emas atau perak yang disimpan (Ferguson, 2008). Puncak dari abstraksi nilai ini adalah transisi menuju sistem uang fiat pada abad ke-20, di mana mata uang tidak lagi dijamin oleh komoditas fisik, melainkan nilainya didasarkan pada kepercayaan (*trust*) terhadap pemerintah yang menerbitkannya dan statusnya sebagai alat pembayaran yang sah (*legal tender*). Sistem ini memberikan fleksibilitas luar biasa bagi negara untuk mengelola kebijakan moneter, namun juga memindahkan fondasi nilai dari yang konkret (komoditas) menjadi abstrak (kepercayaan).

2. Peran Bank Sentral dan Lembaga Keuangan

Dalam ekosistem uang fiat, bank sentral memegang peranan sebagai pilar utama stabilitas moneter dan keuangan. Institusi ini memiliki mandat untuk mengendalikan jumlah uang beredar, mengatur suku bunga, dan menjaga stabilitas harga melalui berbagai instrumen kebijakan moneter (Mishkin, 2019). Selain itu, bank sentral juga berfungsi sebagai *lender of last resort*, yaitu penyedia likuiditas terakhir bagi bank-bank komersial yang mengalami kesulitan untuk mencegah krisis sistemik. Peran ini menempatkan bank sentral sebagai pusat dari sistem keuangan yang sangat tersentralisasi.

Lembaga keuangan lainnya, seperti bank komersial, perusahaan investasi, dan asuransi, bertindak sebagai perantara (*intermediaries*) yang mengalirkan dana dari unit surplus (penabung) ke unit defisit (peminjam). Mereka memfasilitasi alokasi modal, manajemen risiko, dan mekanisme pembayaran dalam perekonomian (Levine, 2005). Struktur hierarkis ini, dengan bank sentral di puncaknya, telah terbukti mampu mendukung

pertumbuhan ekonomi global selama beberapa dekade. Namun, konsentrasi kekuasaan dan informasi pada segelintir institusi ini juga menciptakan risiko moral (*moral hazard*) dan potensi kegagalan sistemik yang dampaknya sangat luas.

3. Krisis Keuangan Global dan Dorongan Inovasi Digital

Krisis Keuangan Global 2008 menjadi titik balik yang mengekspos kerentanan fundamental dari sistem keuangan tersentralisasi. Krisis yang dipicu oleh gelembung kredit perumahan (*subprime mortgage*) di Amerika Serikat ini dengan cepat menyebar ke seluruh dunia, menyebabkan kegagalan institusi keuangan raksasa, resesi ekonomi global, dan hilangnya kepercayaan publik terhadap bank dan regulator (Acharya et al., 2009). Krisis ini menunjukkan bagaimana kebijakan yang salah, manajemen risiko yang buruk, dan kurangnya transparansi pada lembaga-lembaga terpusat dapat menimbulkan konsekuensi katastrofik.

Sebagai respons langsung terhadap krisis ini, muncul gelombang ketidakpercayaan terhadap institusi keuangan tradisional. Di tengah atmosfer inilah, sebuah dokumen berjudul "*Bitcoin: A Peer-to-Peer Electronic Cash System*" dipublikasikan oleh entitas anonim bernama Satoshi Nakamoto pada Oktober 2008 (Nakamoto, 2008). Dokumen ini tidak hanya mengusulkan sebuah mata uang digital, tetapi juga sebuah sistem keuangan alternatif yang tidak memerlukan perantara terpercaya (*trusted third party*). Momentum yang diciptakan oleh krisis 2008 menjadi lahan subur bagi gagasan radikal ini untuk tumbuh, menawarkan sebuah visi sistem keuangan yang lebih transparan, tahan sensor, dan terdesentralisasi.

4. Munculnya Konsep Keuangan Terdesentralisasi (DeFi)

Jika Bitcoin adalah manifestasi pertama dari sistem pembayaran terdesentralisasi, maka Keuangan Terdesentralisasi atau *Decentralized Finance* (DeFi) adalah evolusi lanjutannya yang bertujuan untuk mereplikasi seluruh spektrum layanan keuangan tradisional di atas teknologi *blockchain*. DeFi merujuk pada ekosistem aplikasi keuangan yang dibangun di atas jaringan *blockchain* publik, terutama Ethereum, yang memungkinkan pengguna untuk meminjam, meminjamkan, berdagang, dan mendapatkan bunga atas aset digital mereka tanpa bergantung pada perantara seperti bank (Schär, 2021).

Konsep ini didasarkan pada penggunaan *smart contracts* (kontrak pintar), yaitu program komputer yang secara otomatis mengeksekusi ketentuan perjanjian ketika kondisi tertentu terpenuhi. Dengan DeFi, fungsi-fungsi yang sebelumnya dijalankan oleh bank dan lembaga keuangan kini dapat diotomatisasi dan diakses oleh siapa saja yang memiliki koneksi internet. Kemunculan DeFi menandai pergeseran paradigma dari sistem yang berbasis pada institusi menjadi sistem yang berbasis pada kode (*code-based system*), yang menawarkan potensi inklusi keuangan yang lebih besar namun juga menghadirkan tantangan regulasi dan keamanan yang baru (Werner et al., 2022).

B. Definisi dan Konsep Dasar Cryptocurrency

Setelah memetakan konteks historis yang melahirkan inovasi keuangan digital, sub-bab ini akan membedah fondasi teknis dan konseptual dari *cryptocurrency*. Tujuannya adalah untuk memberikan pemahaman yang jernih dan presisi mengenai apa itu *cryptocurrency*, bagaimana ia beroperasi, dan apa yang membedakannya dari bentuk aset digital lainnya. Pembahasan akan dimulai dari definisi fundamental *cryptocurrency*, dilanjutkan dengan penjelasan mengenai teknologi *blockchain* sebagai infrastruktur dasarnya, peran vital kriptografi dalam mengamankan jaringan, serta klasifikasi aset digital seperti koin dan token.

1. Apa itu Cryptocurrency?

Cryptocurrency, atau mata uang kripto, adalah aset digital yang dirancang untuk berfungsi sebagai medium pertukaran yang menggunakan kriptografi kuat untuk mengamankan transaksi keuangan, mengontrol penciptaan unit tambahan, dan memverifikasi transfer aset (Antonopoulos, 2017). Berbeda dengan mata uang fiat yang bersifat sentralistik dan dikeluarkan oleh bank sentral, mayoritas *cryptocurrency* beroperasi dalam sebuah sistem yang terdesentralisasi. Desentralisasi ini dicapai melalui teknologi *Distributed Ledger Technology* (DLT), di mana *blockchain* adalah bentuk yang paling umum.

Secara esensial, *cryptocurrency* adalah entri data dalam sebuah basis data (*database*) terdistribusi yang tidak dapat diubah oleh siapa pun tanpa memenuhi kondisi tertentu. Aset ini tidak memiliki wujud fisik dan hanya

ada di dalam jaringan. Nilainya, seperti halnya aset lainnya, ditentukan oleh mekanisme pasar, yaitu penawaran dan permintaan (Brito & Castillo, 2013). Karakteristik utamanya meliputi desentralisasi, transparansi (semua transaksi tercatat di buku besar publik), dan imutabilitas (*immutability*), yang berarti sekali transaksi tercatat, ia tidak dapat diubah atau dihapus.

2. Teknologi Blockchain sebagai Tulang Punggung

Blockchain (rantai blok) adalah teknologi buku besar terdistribusi yang menjadi dasar bagi hampir semua *cryptocurrency*. Teknologi ini dapat dibayangkan sebagai sebuah buku catatan digital yang dibagikan kepada seluruh peserta dalam jaringan (disebut *nodes*). Setiap catatan transaksi dikelompokkan ke dalam sebuah "blok". Setiap blok baru yang dibuat akan terhubung secara kriptografis dengan blok sebelumnya, membentuk sebuah "rantai" yang kronologis dan tidak dapat diubah (Narayanan et al., 2016). Kaitan kriptografis ini, yang menggunakan fungsi *hash*, memastikan integritas seluruh rantai; mengubah satu blok akan secara otomatis membatalkan semua blok berikutnya, yang akan segera terdeteksi oleh jaringan.

Keunggulan utama *blockchain* adalah kemampuannya untuk menciptakan kepercayaan (*trust*) dalam lingkungan yang tidak memiliki otoritas pusat (*trustless environment*). Kepercayaan tidak lagi ditempatkan pada satu institusi, melainkan didistribusikan ke seluruh jaringan melalui mekanisme konsensus, seperti *Proof-of-Work* (PoW) pada Bitcoin atau *Proof-of-Stake* (PoS) pada versi terbaru Ethereum (Buterin, 2014). Mekanisme ini memastikan bahwa semua peserta menyetujui versi buku besar yang sama, sehingga mencegah masalah pengeluaran ganda (*double-spending*) tanpa memerlukan perantara.

3. Kriptografi: Mengamankan Transaksi Digital

Kriptografi adalah ilmu dan seni menjaga kerahasiaan pesan, dan dalam konteks *cryptocurrency*, perannya sangat fundamental untuk memastikan keamanan, otentikasi, dan integritas. Dua konsep kriptografi utama yang digunakan adalah *hashing* dan kriptografi kunci publik (*public-key cryptography*). *Hashing* adalah proses mengubah data input dengan ukuran berapa pun menjadi output dengan ukuran tetap yang disebut

hash. Fungsi ini bersifat satu arah, artinya sangat sulit untuk merekayasa balik data asli dari *hash*-nya. Dalam *blockchain*, *hashing* digunakan untuk menghubungkan blok dan memastikan integritas data (Antonopoulos, 2017).

Sementara itu, kriptografi kunci publik adalah fondasi dari kepemilikan dan otorisasi transaksi. Setiap pengguna memiliki sepasang kunci: *public key* (kunci publik) dan *private key* (kunci pribadi). *Public key* dapat dibagikan secara bebas dan berfungsi sebagai alamat untuk menerima dana, mirip dengan nomor rekening bank. Sebaliknya, *private key* harus dijaga kerahasiaannya dan berfungsi sebagai "tanda tangan digital" untuk mengotorisasi transaksi keluar dari alamat tersebut (Narayanan et al., 2016). Kepemilikan *private key* secara efektif adalah kepemilikan atas aset kripto yang tersimpan di alamat tersebut.

4. Perbedaan antara Koin, Token, dan Aset Digital

Meskipun sering digunakan secara bergantian, istilah "koin" dan "token" memiliki perbedaan teknis yang signifikan dalam ekosistem aset digital.

a. Koin (*Coin*): Sebuah aset digital yang beroperasi di atas *blockchain*-nya sendiri (*native blockchain*). Contoh paling jelas adalah Bitcoin (BTC) yang berjalan di *blockchain* Bitcoin, dan Ether (ETH) yang merupakan koin asli dari *blockchain* Ethereum. Koin biasanya berfungsi sebagai "bahan bakar" atau alat pembayaran biaya transaksi di dalam jaringannya masing-masing.
b. Token: Sebuah aset digital yang tidak memiliki *blockchain* sendiri, melainkan "menumpang" atau dibangun di atas *blockchain* yang sudah ada, seperti Ethereum (dengan standar token ERC-20), Solana, atau Binance Smart Chain (Binance, 2022). Token dapat merepresentasikan berbagai hal, mulai dari utilitas (hak akses ke sebuah layanan), sekuritas (saham perusahaan), hingga aset dunia nyata (*real-world asset*).
c. Aset Digital (*Digital Asset*): Ini adalah istilah payung yang lebih luas, mencakup koin, token, dan bentuk aset digital lainnya yang diamankan secara kriptografis, seperti *Non-Fungible Tokens* (NFTs) yang merepresentasikan kepemilikan unik atas item digital atau fisik.

C. Lanskap Ekonomi Digital di Indonesia

Sub-bab ini mengalihkan fokus analisis ke konteks domestik, yaitu Indonesia, untuk membedah dinamika, potensi, dan tantangan ekonomi digital nasional. Pertumbuhan pesat penetrasi internet telah menjadi katalisator utama bagi transformasi digital di berbagai sektor. Bagian ini akan mengkaji skala pertumbuhan tersebut, peran pilar-pilar utama seperti *e-commerce* dan *fintech*, respons awal pemerintah dalam merumuskan kerangka regulasi untuk aset kripto, serta mengidentifikasi peluang dan hambatan yang dihadapi Indonesia dalam memaksimalkan potensi ekonomi digitalnya.

1. Pertumbuhan Pengguna Internet dan Transaksi Digital

Indonesia telah mengalami ledakan digital dalam dekade terakhir. Data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) secara konsisten menunjukkan peningkatan penetrasi internet yang signifikan, melampaui 78% dari total populasi pada tahun 2023 (APJII, 2023). Pertumbuhan ini, yang didominasi oleh pengguna perangkat seluler, telah mengubah secara drastis perilaku konsumen dan menciptakan pasar digital yang masif. Peningkatan ini berkorelasi langsung dengan lonjakan volume dan nilai transaksi digital.

Laporan dari Bank Indonesia menunjukkan bahwa nilai transaksi uang elektronik dan perbankan digital terus mencatatkan rekor baru setiap tahunnya, menandakan pergeseran preferensi masyarakat dari transaksi tunai ke nontunai (Bank Indonesia, 2023). Fenomena ini menciptakan fondasi yang kuat bagi adopsi inovasi keuangan yang lebih lanjut, termasuk aset kripto, karena masyarakat menjadi semakin terbiasa dengan konsep aset dan transaksi yang tidak berwujud fisik.

2. Peran E-commerce, Fintech, dan Ekonomi Gig

Tiga pilar utama yang menopang dan mengakselerasi ekonomi digital Indonesia adalah *e-commerce*, *fintech* (teknologi finansial), dan *gig economy*. Platform *e-commerce* seperti Tokopedia, Shopee, dan Lazada telah merevolusi sektor ritel, memberikan akses pasar yang lebih luas bagi jutaan Usaha Mikro, Kecil, dan Menengah (UMKM). Keberhasilan mereka tidak hanya terletak pada perdagangan barang, tetapi juga dalam

membangun ekosistem pembayaran digital yang terintegrasi (Google, Temasek, & Bain & Company, 2022).

Di sisi lain, sektor *fintech* telah mengisi celah yang tidak terlayani oleh lembaga keuangan tradisional, terutama dalam hal pinjaman (*peer-to-peer lending*), pembayaran digital (*e-wallet*), dan investasi ritel. Sementara itu, *gig economy*, yang difasilitasi oleh platform seperti Gojek dan Grab, telah menciptakan model pekerjaan baru yang fleksibel. Sinergi antara ketiga pilar ini tidak hanya mendorong pertumbuhan ekonomi, tetapi juga mempercepat literasi dan inklusi keuangan digital di seluruh lapisan masyarakat.

3. Regulasi Awal Pemerintah Terhadap Aset Kripto

Respons pemerintah Indonesia terhadap kemunculan aset kripto pada awalnya diwarnai oleh kehati-hatian. Bank Indonesia secara konsisten melarang penggunaan *cryptocurrency* sebagai alat pembayaran yang sah, sejalan dengan Undang-Undang Mata Uang yang menetapkan Rupiah sebagai satu-satunya alat pembayaran legal di wilayah NKRI (Bank Indonesia, 2018). Namun, pemerintah melihat potensi aset kripto sebagai komoditas yang dapat diperdagangkan.

Pada tahun 2019, Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) mengeluarkan peraturan yang secara resmi mengakui aset kripto sebagai komoditas yang dapat menjadi subjek kontrak berjangka, sehingga memberikan landasan hukum bagi perdagangan aset kripto di bursa-bursa yang terdaftar (Peraturan Bappebti No. 5 Tahun 2019). Langkah ini menandai pendekatan dualistik: melarang sebagai alat bayar, namun melegalkan sebagai aset investasi. Regulasi awal ini, meskipun penting, masih terus berkembang seiring dengan kompleksitas pasar dan risiko yang muncul.

4. Potensi dan Tantangan Ekonomi Digital Nasional

Potensi ekonomi digital Indonesia sangat besar, didorong oleh populasi muda yang melek teknologi dan pasar domestik yang luas. Potensi ini mencakup peningkatan efisiensi ekonomi, penciptaan lapangan kerja baru, dan percepatan inklusi keuangan. Aset kripto dan teknologi *blockchain* berpotensi lebih lanjut untuk membuka inovasi di bidang remitansi, pembiayaan UMKM, dan transparansi rantai pasok (World Bank, 2021).

Namun, potensi ini diimbangi oleh tantangan yang signifikan. Kesenjangan digital (*digital divide*) antara wilayah perkotaan dan perdesaan masih menjadi isu utama. Tingkat literasi digital dan keuangan yang belum merata membuat masyarakat rentan terhadap penipuan dan investasi bodong. Dari sisi regulasi, pemerintah dihadapkan pada tugas berat untuk menciptakan kerangka kerja yang dapat mendorong inovasi sambil memitigasi risiko stabilitas keuangan, perlindungan konsumen, dan potensi aktivitas ilegal.

D. Permasalahan Utama: Kejahatan Ekonomi Digital

Seiring dengan pertumbuhan eksponensial ekonomi digital, muncul pula sisi gelapnya: peningkatan volume dan kecanggihan kejahatan ekonomi digital. Sub-bab ini akan mengidentifikasi dan mendefinisikan permasalahan utama yang menjadi fokus sentral buku ini. Pembahasan akan mencakup ruang lingkup kejahatan ekonomi digital yang difasilitasi oleh *cryptocurrency*, dampaknya terhadap stabilitas sistemik dan keamanan publik, tantangan unik yang dihadapi penegak hukum, dan diakhiri dengan penegasan urgensi untuk menganalisis fenomena ini melalui lensa hukum pidana Islam.

1. Definisi dan Ruang Lingkup Kejahatan Ekonomi Digital

Kejahatan ekonomi digital, dalam konteks buku ini, didefinisikan sebagai setiap tindakan ilegal yang memanfaatkan infrastruktur digital—termasuk internet, komputer, dan teknologi *blockchain*—untuk memperoleh keuntungan finansial secara tidak sah. Sifat anonimitas atau pseudo-anonimitas *cryptocurrency* menjadikannya medium yang menarik untuk berbagai aktivitas kriminal. Ruang lingkupnya sangat luas, mencakup:

a. Penipuan (*Fraud dan Scams*): Skema Ponzi dan piramida berbasis kripto, penawaran koin perdana palsu (*fake ICOs*), dan skema *rug pull* di mana pengembang proyek melarikan diri dengan dana investor.
b. Pencucian Uang (*Money Laundering*): Penggunaan *mixer* atau *tumbler* kripto untuk mengaburkan jejak dana hasil kejahatan, seperti perdagangan narkotika, korupsi, atau pendanaan terorisme (FATF, 2021).

c. Peretasan dan Pencurian (*Hacking and Theft*): Serangan terhadap bursa aset kripto, dompet digital (*wallets*), atau protokol DeFi untuk mencuri dana pengguna.

d. Pasar Gelap Daring (*Darknet Markets*): Penggunaan *cryptocurrency* sebagai alat pembayaran utama untuk barang dan jasa ilegal di *dark web*.

2. Ancaman Terhadap Stabilitas Keuangan dan Keamanan Publik

Kejahatan ekonomi digital bukan hanya merugikan individu, tetapi juga membawa ancaman sistemik. Skala pencucian uang yang besar melalui aset kripto dapat merusak integritas sistem keuangan nasional dan global (FATF, 2021). Aliran dana ilegal ini dapat mendistorsi data ekonomi dan mempersulit otoritas moneter dalam merumuskan kebijakan yang efektif. Volatilitas ekstrem yang sering dipicu oleh manipulasi pasar juga dapat menciptakan risiko stabilitas jika eksposur lembaga keuangan terhadap aset kripto meningkat tanpa mitigasi risiko yang memadai.

Dari perspektif keamanan publik, penggunaan *cryptocurrency* untuk pendanaan terorisme dan perdagangan barang ilegal merupakan ancaman langsung terhadap keamanan negara. Kemampuan kelompok kriminal untuk memindahkan nilai lintas batas negara dengan cepat dan relatif anonim menantang upaya penegakan hukum konvensional. Selain itu, maraknya penipuan investasi kripto dapat mengikis kepercayaan publik terhadap sistem keuangan secara keseluruhan dan menyebabkan kerugian sosial yang signifikan.

3. Kompleksitas Penegakan Hukum di Dunia Maya

Penegakan hukum terhadap kejahatan ekonomi digital menghadapi kompleksitas yang belum pernah terjadi sebelumnya. Sifat *cryptocurrency* yang lintas batas (*borderless*) menimbulkan tantangan yurisdiksi: kejahatan dapat dilakukan oleh pelaku di satu negara, terhadap korban di negara lain, dengan menggunakan server yang berlokasi di negara ketiga. Hal ini mempersulit proses investigasi, pengumpulan bukti, dan ekstradisi pelaku (Choo, 2015).

Selain itu, teknologi yang dirancang untuk meningkatkan privasi, seperti *mixer* dan *privacy coins* (misalnya, Monero), secara aktif digunakan

untuk mengaburkan jejak transaksi, membuatnya sangat sulit untuk dilacak bahkan oleh analis *blockchain* yang berpengalaman. Penegak hukum sering kali tertinggal dalam hal kapasitas teknis dan sumber daya untuk mengimbangi kecepatan inovasi para pelaku kejahatan. Kerjasama internasional menjadi krusial, namun sering kali terhambat oleh perbedaan kerangka hukum dan prioritas antar negara.

4. Urgensi Kajian dari Perspektif Hukum Pidana Islam

Di tengah kompleksitas teknologi dan tantangan penegakan hukum modern, perspektif hukum pidana Islam (*jināyah*) menawarkan kerangka kerja etis dan yuridis yang relevan. Hukum Islam menempatkan penekanan kuat pada perlindungan properti (*ḥifẓ al-māl*), keadilan (*al-ʿadl*), dan pencegahan kerusakan (*mafsadah*). Kejahatan seperti penipuan (*ghishsh*, *tadlīs*), pencurian (*sariqah*), dan perampasan harta secara tidak sah (*aklu amwāl al-nās bi al-bāṭil*) memiliki padanan konseptual yang kuat dalam fikih (Auda, 2008).

Urgensi kajian ini terletak pada kebutuhan untuk merumuskan respons hukum yang tidak hanya bersifat teknis-positivistik, tetapi juga berakar pada prinsip-prinsip keadilan substantif yang diakui oleh mayoritas penduduk Indonesia. Menganalisis kejahatan ekonomi digital melalui lensa hukum pidana Islam dapat memberikan legitimasi moral dan sosial bagi upaya penegakan hukum, serta menawarkan prinsip-prinsip untuk merumuskan hukuman yang bersifat preventif (*zawājir*) dan korektif (*jawābir*). Kajian ini menjadi penting untuk menjawab bagaimana sistem hukum yang berakar pada tradisi dapat beradaptasi untuk mengatasi kejahatan yang lahir dari teknologi paling mutakhir.

Ruang Lingkup

Bagian penutup dari bab pengantar ini bertujuan untuk memaparkan kerangka metodologis dan batasan penelitian yang akan memandu seluruh pembahasan dalam buku ini. Dengan menjelaskan pendekatan penelitian, sumber data yang digunakan, batasan masalah yang ditetapkan, dan sistematika penulisan, sub-bab ini memberikan peta jalan yang jelas bagi pembaca untuk mengikuti alur argumen dan memahami ruang lingkup analisis yang dilakukan.

1. Pendekatan Penelitian: Yuridis-Normatif dan Studi Kasus

Penelitian ini menggunakan pendekatan utama yuridis-normatif, yang berfokus pada analisis terhadap norma, asas, dan doktrin hukum, khususnya dalam lingkup hukum pidana Islam. Pendekatan ini melibatkan inventarisasi, interpretasi, dan sistematisasi hukum positif (regulasi pemerintah terkait aset kripto) dan hukum Islam (Al-Qur'an, Sunnah, dan ijtihad para ulama) untuk menemukan jawaban atas permasalahan hukum yang diajukan (Soekanto & Mamudji, 2003).

Pendekatan normatif ini akan diperkaya dengan pendekatan studi kasus (*case study*). Beberapa kasus kejahatan ekonomi digital terkemuka yang terjadi di Indonesia atau melibatkan warga negara Indonesia akan dianalisis secara mendalam. Studi kasus ini tidak bertujuan untuk generalisasi statistik, melainkan untuk memberikan ilustrasi konkret mengenai modus operandi kejahatan, kompleksitas pembuktian, dan bagaimana kerangka hukum pidana Islam dapat diterapkan untuk menganalisis kasus-kasus tersebut.

2. Sumber Data: Literatur, Fatwa, Peraturan, dan Putusan Pengadilan

Sumber data dalam penyusunan buku ini bersifat kualitatif dan berasal dari berbagai sumber primer dan sekunder.

a. Sumber Hukum Islam Primer: Al-Qur'an dan Hadis-hadis yang relevan dengan muamalah, kejahatan terhadap harta, dan penipuan.
b. Sumber Hukum Islam Sekunder: Kitab-kitab fikih klasik dan kontemporer dalam bidang *jināyah* dan *mu'āmalah*, fatwa-fatwa dari lembaga-lembaga Islam otoritatif di tingkat nasional (seperti MUI) dan internasional, serta artikel jurnal ilmiah tentang hukum Islam dan keuangan digital.
c. Peraturan Perundang-undangan: Undang-Undang di Indonesia yang relevan, seperti UU ITE, UU TPPU, UU Mata Uang, serta peraturan teknis dari Bappebti dan OJK.
d. Literatur Akademis: Buku, disertasi, dan artikel jurnal internasional bereputasi mengenai *cryptocurrency*, *blockchain*, ekonomi digital, dan *cybercrime*.

e. Putusan Pengadilan: Analisis terhadap putusan pengadilan terkait kasus kejahatan siber dan keuangan (jika tersedia dan relevan) untuk melihat bagaimana hakim menafsirkan dan menerapkan hukum dalam praktik.

3. Batasan Masalah: Fokus pada Hukum Pidana Islam di Indonesia

Untuk menjaga kedalaman dan fokus analisis, buku ini menetapkan batasan masalah yang jelas. Pertama, meskipun pembahasan menyentuh aspek teknis *cryptocurrency* dan ekonomi, fokus utamanya adalah pada perspektif hukum, khususnya hukum pidana. Kedua, dari berbagai mazhab hukum yang ada, analisis akan dipusatkan pada hukum pidana Islam (*fiqh al-jināyah*) sebagai kerangka analisis utama. Ketiga, konteks geografis dan yuridis dibatasi pada Indonesia. Artinya, penerapan dan relevansi hukum pidana Islam akan selalu dikaitkan dengan sistem hukum nasional Indonesia dan tantangan spesifik yang dihadapi di dalam negeri. Buku ini tidak akan membahas secara mendalam aspek hukum perdata atau hukum internasional, kecuali jika bersinggungan langsung dengan analisis pidana.

4. Sistematika Penulisan dan Pembahasan

Buku ini disusun secara sistematis untuk memandu pembaca dari konsep fundamental hingga analisis mendalam. Bab 1 (bab ini) berfungsi sebagai pengantar umum, memetakan lanskap dan permasalahan. Bab 2 akan mendalami konsep *jarīmah* (tindak pidana) dalam hukum pidana Islam dan relevansinya dengan kejahatan siber. Bab 3 akan menganalisis secara spesifik bentuk-bentuk kejahatan ekonomi digital (penipuan, pencucian uang, dll.) melalui kacamata *fiqh al-jināyah*. Bab 4 akan membahas sistem pembuktian dan penjatuhan sanksi (*'uqūbah*) dalam hukum Islam untuk kejahatan-kejahatan tersebut. Terakhir, Bab 5 akan menyajikan sintesis, kesimpulan, dan rekomendasi kebijakan untuk harmonisasi antara penegakan hukum nasional dan prinsip-prinsip hukum pidana Islam dalam menghadapi tantangan ekonomi digital di Indonesia.

Analisis Mendalam Konsep Kunci Bab 1: Evolusi Sistem Keuangan (Sentralisasi vs. Desentralisasi)

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk membingkai kelahiran *cryptocurrency* bukan sebagai sebuah anomali teknologi, melainkan sebagai sebuah respons historis dan filosofis terhadap keterbatasan dan kegagalan sistem keuangan yang ada. Dengan memahami evolusi ini, pembaca dapat melihat *cryptocurrency* (khususnya Bitcoin sebagai pionirnya) sebagai sebuah solusi yang diusulkan untuk masalah-masalah spesifik dalam sistem keuangan terpusat.

Bab 1 menggunakan evolusi ini untuk membangun narasi bahwa setiap sistem keuangan memiliki "cacat" atau masalah yang kemudian mendorong lahirnya sistem berikutnya.

Elemen-Elemen Kunci dalam Evolusi:

1. Perantara (*Intermediary*): Siapa yang memvalidasi dan mencatat transaksi? Apakah ada pihak ketiga yang dipercaya?
2. Basis Kepercayaan (*Trust*): Kepercayaan diletakkan pada apa? Pada individu, institusi, pemerintah, atau pada kode matematika?
3. Sumber Nilai (*Source of Value*): Apa yang membuat "uang" tersebut berharga? Apakah karena kegunaan intrinsiknya, dekrit pemerintah, atau kelangkaan matematis?
4. Titik Kegagalan (*Point of Failure*): Apa risiko utama atau kelemahan inheren dari sistem tersebut?

Analisis Komparatif: Evolusi Sistem Keuangan

Tabel berikut membedah evolusi sistem keuangan dari yang paling primitif hingga ke era desentralisasi, menyoroti pergeseran fundamental pada setiap tahapnya.

Fitur Kunci	Sistem Barter	Uang Komoditas (Emas, Perak)	Uang Fiat (Terpusat)	Cryptocurrency (Terdesentralisasi)
Definisi	Pertukaran langsung barang/jasa tanpa medium perantara.	Penggunaan komoditas dengan nilai intrinsik sebagai alat tukar.	Uang yang nilainya didasarkan pada dekrit/ kepercayaan pada pemerintah.	Aset digital yang diamankan oleh kriptografi di jaringan *peer-to-peer*.
Perantara	Tidak Ada. Transaksi langsung antar individu.	Minimal. Mungkin ada penimbang atau penilai keaslian.	Sangat Sentral. Bank, Bank Sentral, Lembaga Kliring.	Tidak Ada. Transaksi divalidasi oleh jaringan komputer (*nodes*).
Basis Kepercayaan	Kepercayaan pada individu lain yang bertransaksi.	Kepercayaan pada nilai intrinsik komoditas itu sendiri (langka, tahan lama).	Kepercayaan pada otoritas pemerintah dan stabilitas Bank Sentral.	Kepercayaan pada kode matematika (protokol) dan kekuatan jaringan (*network effect*).
Sumber Nilai	Kegunaan langsung dari barang/jasa yang ditukar.	Kelangkaan alami, kegunaan industri/ perhiasan.	Dekrit Pemerintah. Dinyatakan sah sebagai alat pembayaran.	Kelangkaan Digital (dibatasi oleh kode), permintaan pasar, dan keamanan jaringan.
Masalah Utama / Titik Kegagalan	Inefisiensi. Sulit menemukan "kesamaan keinginan" (*double coincidence of wants*).	Tidak Praktis. Sulit dibawa, dibagi, dan diverifikasi keasliannya.	Risiko Sentralisasi. Inflasi, sensor, penyalahgunaan wewenang, dan krisis sistemik (cth: Krisis 2008).	Risiko Teknologi & Adopsi. Volatilitas tinggi, skalabilitas, keamanan *private key*, dan potensi penggunaan ilegal.
Contoh Konkret	Menukar beras dengan ikan.	Koin Dinar (emas) dan Dirham (perak).	Rupiah, Dolar AS, Euro.	Bitcoin (BTC), Ethereum (ETH).

Kontribusi Konsep Evolusi dalam Bab 1:

Konsep ini adalah panggung utama tempat semua elemen lain dalam Bab 1 diletakkan.

1. Memberikan Justifikasi Kelahiran Kripto: Dengan menyoroti "Risiko Sentralisasi" pada kolom Uang Fiat, terutama Krisis Keuangan 2008, Bab 1 memberikan argumen kuat bahwa Bitcoin diciptakan sebagai antitesis dari sistem yang dianggap rapuh dan tidak adil tersebut. Dokumen *white paper* Bitcoin yang dirilis pada Oktober 2008 adalah bukti historis dari hal ini.
2. Menjelaskan Teknologi Inti: Konsep "tanpa perantara" dan "kepercayaan pada kode" secara langsung mengarah pada kebutuhan akan teknologi Blockchain dan Kriptografi, yang kemudian dijelaskan di sub-bab 1.2.
3. Membingkai Masalah Kejahatan: Tabel ini juga secara implisit menunjukkan mengapa *cryptocurrency* menarik untuk kejahatan. Fitur "tanpa perantara" dan basis kepercayaan pada kode (bukan pada identitas) menciptakan sifat pseudenonim yang dapat dieksploitasi, yang menjadi pengantar bagi sub-bab 1.4 tentang masalah kejahatan ekonomi digital.

BAB 2

Konsep Kejahatan (Jarimah) dalam Hukum Pidana Islam

Setelah Bab 1 memaparkan lanskap teknologi dan ekonomi yang melahirkan kejahatan digital, Bab 2 beralih ke jantung kerangka analisis buku ini: hukum pidana Islam. Dalam konstelasi studi hukum, *fiqh al-jināyah* sering kali dipahami secara parsial, terbatas pada pembahasan sanksi fisik tanpa mengapresiasi filsafat dan struktur logis yang melandasinya. Bab ini memposisikan hukum pidana Islam bukan sebagai korpus hukum yang statis, melainkan sebagai sebuah sistem yuridis-etis yang dinamis. *Research gap* yang hendak dijembatani adalah kurangnya literatur akademis berbahasa Indonesia yang secara sistematis mengartikulasikan konsep-konsep fundamental *jināyah* (seperti klasifikasi *jarīmah*, unsur-unsur pidana, dan asas legalitas) dan secara langsung menghubungkannya dengan tantangan kejahatan kontemporer. Dengan demikian, pertanyaan penelitian utama yang akan dijawab oleh bab ini adalah: Bagaimana prinsip, klasifikasi, dan unsur-unsur kejahatan dalam hukum pidana Islam dapat membentuk sebuah kerangka kerja yang valid dan aplikatif untuk menganalisis kejahatan ekonomi digital di era modern?

A. Pengantar Filsafat Hukum Pidana Islam (Jinayah)

Sub-bab ini bertujuan untuk meletakkan fondasi filosofis yang menopang seluruh bangunan hukum pidana Islam. Pemahaman terhadap *jināyah* tidak akan lengkap tanpa memahami tujuan luhur di baliknya. Oleh karena itu, analisis akan dimulai dari *Maqāshid al-Sharī'ah* sebagai jiwa dari legislasi Islam. Selanjutnya, akan dibahas prinsip-prinsip universal seperti keadilan dan kemanusiaan yang menjadi ciri khasnya, diikuti dengan identifikasi sumber-sumber hukum otoritatifnya, dan diakhiri dengan perbandingan mendasar dengan sistem hukum pidana konvensional untuk menajamkan pemahaman atas karakteristik uniknya.

1. Tujuan Syariah (Maqashid al-Shari'ah) sebagai Dasar

Filsafat hukum pidana Islam secara inheren terikat pada konsep *Maqāshid al-Sharī'ah*, yaitu tujuan-tujuan esensial di balik penetapan hukum syariah. Menurut para yuris Islam terkemuka seperti Imam al-Ghazali dan al-Syatibi, tujuan utama syariah adalah untuk mewujudkan kemaslahatan (*jalb al-maṣāliḥ*) dan menolak kerusakan (*dar' al-mafāsid*) bagi umat manusia di dunia dan akhirat. Kemaslahatan ini diklasifikasikan ke dalam lima nilai universal yang wajib dilindungi (*al-ḍarūriyyāt al-*

khamsah): perlindungan terhadap agama (*ḥifẓ al-dīn*), jiwa (*ḥifẓ al-nafs*), akal (*ḥifẓ al-ʿaql*), keturunan (*ḥifẓ al-nasl*), dan harta (*ḥifẓ al-māl*) (Auda, 2008). Hukum pidana Islam, dengan segala bentuk sanksinya, berfungsi sebagai "benteng" untuk melindungi kelima nilai fundamental ini dari segala bentuk ancaman dan pelanggaran.

2. Prinsip Keadilan, Kemanusiaan, dan Kepastian Hukum

Hukum pidana Islam ditegakkan di atas beberapa prinsip fundamental. Pertama, prinsip keadilan (*al-ʿadl*), yang menuntut agar hukuman setimpal dengan kejahatan dan tidak ada seorang pun yang dihukum atas kesalahan orang lain (Al-Qur'an, Al-An'am: 164). Keadilan juga berarti memberikan hak kepada korban, baik melalui retribusi (*qiṣāṣ*) maupun kompensasi (*diyat*). Kedua, prinsip kemanusiaan, yang tercermin dalam larangan menjatuhkan hukuman yang melampaui batas dan anjuran kuat untuk memaafkan dalam kasus *qiṣāṣ*. Ketiga, prinsip kepastian hukum, yang terwujud dalam asas legalitas (*la jarīmah wa la 'uqubah illa bi nash*), yang berarti suatu perbuatan tidak dapat dianggap kejahatan dan tidak dapat dihukum kecuali ada dalil (*nash*) yang melarangnya. Prinsip ini memberikan jaminan dan perlindungan bagi individu dari kesewenang-wenangan penguasa (Al-Zuhaili, 2003).

3. Sumber Hukum: Al-Qur'an, Sunnah, Ijma', dan Qiyas

Otoritas hukum pidana Islam bersumber dari hierarki dalil yang telah disepakati. Al-Qur'an adalah sumber primer dan tertinggi, yang berisi ayat-ayat yang menetapkan larangan dan sanksi untuk kejahatan-kejahatan tertentu. Sunnah, yaitu perkataan, perbuatan, dan ketetapan Nabi Muhammad SAW, berfungsi sebagai penjelas dan perinci dari Al-Qur'an, serta menetapkan hukum-hukum yang tidak disebutkan dalam Al-Qur'an. Ijmā', atau konsensus para ulama mujtahid setelah wafatnya Nabi, menjadi sumber hukum yang mengikat pada persoalan yang tidak memiliki dalil tegas dalam Al-Qur'an dan Sunnah. Terakhir, Qiyās, yaitu penalaran analogis, digunakan untuk menetapkan hukum suatu kasus baru dengan cara membandingkannya dengan kasus lama yang sudah ada hukumnya karena adanya kesamaan *'illah* (alasan hukum) (Hallaq, 2009). Keempat sumber ini membentuk kerangka kerja metodologis bagi para yuris untuk menggali hukum (*istinbāṭ al-aḥkām*).

4. Perbedaan Mendasar dengan Hukum Pidana Konvensional

Meskipun memiliki beberapa kesamaan tujuan (seperti menjaga ketertiban), hukum pidana Islam memiliki perbedaan filosofis yang mendasar dengan hukum pidana konvensional (positivistik). Pertama, sumber legitimasi: hukum pidana Islam bersumber dari wahyu Ilahi (transendental), sementara hukum konvensional bersumber dari kedaulatan negara atau kontrak sosial (antroposentris). Kedua, orientasi hukuman: sanksi dalam Islam (*'uqūbah*) memiliki dimensi ganda, yaitu sebagai penebus dosa di akhirat (*kawāffir*) dan sebagai pencegah di dunia (*zawājir*), sementara hukum konvensional murni berorientasi pada efek jera, rehabilitasi, atau retribusi di dunia. Ketiga, ruang lingkup: hukum Islam mencakup perbuatan yang melanggar hak Allah (misalnya, murtad, minum khamr) dan hak manusia, sedangkan hukum konvensional umumnya hanya berfokus pada pelanggaran hak manusia dan ketertiban umum (Bassiouni, 1982).

B. Klasifikasi Tindak Pidana (Jarimah)

Untuk memahami bagaimana hukum pidana Islam beroperasi, penting untuk mengetahui bagaimana ia mengklasifikasikan berbagai jenis tindak pidana. Klasifikasi ini tidak hanya bersifat akademis, tetapi juga memiliki implikasi langsung terhadap jenis sanksi dan prosedur peradilannya. Sub-bab ini akan menguraikan tiga kategori utama *jarīmah*: *hudūd*, *qiṣāṣ-diyat*, dan *ta'zīr*. Pembahasan akan diakhiri dengan analisis mengenai bagaimana klasifikasi tripartit ini tetap relevan dan dapat diterapkan untuk mengkategorikan kejahatan-kejahatan di era digital.

1. Jarimah Hudud: Kejahatan dengan Sanksi Tertentu dari Nash

Jarīmah hudūd adalah kategori tindak pidana yang paling serius, didefinisikan sebagai kejahatan yang bentuk dan kadar sanksinya telah ditetapkan secara spesifik oleh Al-Qur'an atau Sunnah. Sanksi ini dianggap sebagai "hak Allah" (*ḥaqq Allāh*), yang berarti tidak ada ruang bagi hakim, penguasa, atau bahkan korban untuk mengubah, mengurangi, atau memaafkannya setelah kasusnya sampai ke pengadilan. Kejahatan yang termasuk dalam kategori ini adalah pencurian (*sariqah*), perampokan (*ḥirābah*), perzinaan (*zinā*), menuduh orang lain berzina tanpa bukti (*qażf*), dan meminum minuman keras (*syurb al-khamr*) (Al-Mawardi, 1996).

Prosedur pembuktian untuk *jarīmah hudūd* sangat ketat untuk memastikan tidak ada keraguan sedikit pun (*syubhat*) dalam penjatuhan sanksi.

2. Jarimah Qisas-Diyat: Kejahatan Terhadap Jiwa dan Badan

Jarīmah qiṣāṣ-diyat adalah tindak pidana yang berkaitan dengan serangan terhadap jiwa dan integritas fisik manusia, seperti pembunuhan dan penganiayaan. Sanksi utamanya adalah *qiṣāṣ*, yaitu hukuman balasan yang setimpal (misalnya, nyawa dibalas nyawa). Namun, kejahatan ini dianggap sebagai "hak manusia" (*ḥaqq al-ādamī*), yang memberikan korban atau keluarganya hak untuk memilih antara tiga opsi: menuntut *qiṣāṣ*, memaafkan dan menerima kompensasi finansial (*diyat*), atau memaafkan sepenuhnya tanpa kompensasi (Oudah, 2007). Fleksibilitas ini menunjukkan penekanan hukum Islam pada pemulihan hubungan sosial dan hak-hak korban.

3. Jarimah Ta'zir: Kejahatan dengan Sanksi Berdasarkan Kebijakan Penguasa (Ulil Amri)

Jarīmah ta'zīr adalah kategori tindak pidana yang paling luas dan fleksibel. Kategori ini mencakup semua perbuatan maksiat atau terlarang yang tidak termasuk dalam kategori *hudūd* atau *qiṣāṣ-diyat*. Jenis perbuatan dan sanksinya tidak ditetapkan secara spesifik oleh *nash*, melainkan diserahkan kepada kebijakan (*ijtihād*) penguasa atau lembaga legislatif (*ulil amri*) untuk menentukannya demi kemaslahatan umum (Al-Zuhaili, 2003). Sanksi *ta'zīr* memiliki rentang yang sangat lebar, mulai dari teguran, denda, penjara, hingga hukuman fisik, yang disesuaikan dengan tingkat keparahan kejahatan dan kondisi pelaku. Kategori inilah yang memberikan dinamisme pada hukum pidana Islam untuk merespons perkembangan zaman dan munculnya bentuk-bentuk kejahatan baru.

4. Relevansi Klasifikasi Jarimah di Era Digital

Klasifikasi tripartit ini memiliki relevansi yang tinggi dalam menghadapi kejahatan ekonomi digital. Sebagian besar kejahatan siber, seperti penipuan daring (*online fraud*), peretasan (*hacking*), penyebaran disinformasi, dan pencucian uang, secara alami masuk ke dalam kategori *jarīmah ta'zīr*. Hal ini karena bentuk-bentuk kejahatan ini tidak secara eksplisit disebutkan dalam *nash* sebagai kejahatan *hudūd* atau *qiṣāṣ*. Dengan demikian,

pemerintah (sebagai *ulil amri*) memiliki wewenang dan kewajiban untuk menetapkan undang-undang (seperti UU ITE dan UU TPPU) yang melarang perbuatan-perbuatan tersebut dan menentukan sanksi yang dianggap efektif dan adil, selama tidak bertentangan dengan prinsip-prinsip syariah. Beberapa kejahatan, seperti pencurian aset kripto dari dompet digital, dapat dianalogikan (*qiyās*) dengan *sariqah* (pencurian *hudūd*), namun sering kali terkendala pemenuhan syarat-syarat formalnya, sehingga lebih praktis untuk dikategorikan sebagai *ta'zīr* (Kamali, 2000).

C. Unsur-Unsur Tindak Pidana dalam Islam

Sebuah perbuatan tidak dapat serta-merta dianggap sebagai *jarīmah* hanya karena terlihat buruk. Hukum pidana Islam, serupa dengan sistem hukum modern, mensyaratkan terpenuhinya unsur-unsur tertentu. Sub-bab ini akan menguraikan tiga rukun atau unsur fundamental yang harus ada agar suatu perbuatan dapat dikualifikasikan sebagai tindak pidana: rukun formal (legalitas), rukun materiil (perbuatan), dan rukun moril (kesalahan). Pemahaman terhadap ketiga unsur ini krusial untuk melakukan analisis hukum yang presisi terhadap kasus-kasus kejahatan modern.

1. Rukun Formal (Al-Rukn al-Syar'i): Adanya Larangan dalam Nash

Rukun pertama dan utama adalah rukun formal atau legalitas, yang sejalan dengan asas legalitas. Rukun ini mensyaratkan bahwa harus ada dalil hukum (*nash*) dari Al-Qur'an, Sunnah, atau produk legislasi *ulil amri* yang sah (dalam kasus *ta'zīr*) yang secara tegas melarang perbuatan tersebut. Tanpa adanya landasan hukum yang melarang, suatu perbuatan, seburuk apa pun secara moral, tidak dapat dituntut secara pidana (Oudah, 2007). Rukun ini adalah jaminan fundamental hak asasi manusia dalam Islam, melindungi individu dari tuntutan hukum yang sewenang-wenang. Untuk kejahatan siber, rukun ini dipenuhi melalui undang-undang yang ditetapkan oleh pemerintah.

2. Rukun Materiil (Al-Rukn al-Maddi): Adanya Perbuatan dan Akibat

Rukun materiil terdiri dari tiga komponen: (1) adanya perbuatan (*fi'l*), baik dalam bentuk tindakan aktif (komisi) maupun pembiaran (omisi); (2) adanya akibat (*natījah*) yang dilarang oleh hukum, seperti hilangnya

harta atau rusaknya reputasi; dan (3) adanya hubungan kausalitas (*'alāqah sababiyyah*) antara perbuatan dan akibat tersebut (Al-Zuhaili, 2003). Dalam kasus penipuan investasi kripto, misalnya, perbuatannya adalah membuat janji palsu, akibatnya adalah hilangnya dana investor, dan harus ada bukti bahwa hilangnya dana tersebut disebabkan langsung oleh janji palsu si pelaku.

3. Rukun Moril (Al-Rukn al-Adabi): Kesalahan (Niat dan Kelalaian)

Rukun moril berkaitan dengan kondisi psikologis pelaku saat melakukan perbuatan, atau yang dikenal dengan konsep "kesalahan". Ini adalah elemen yang menghubungkan perbuatan materiil dengan pertanggungjawaban pribadi pelaku. Kesalahan dapat berbentuk kesengajaan (*'amd* atau *qaṣd jinā'ī*), di mana pelaku mengetahui perbuatannya dilarang dan menghendaki terjadinya akibat dari perbuatannya tersebut. Bentuk kedua adalah ketidaksengajaan atau kelalaian (*khata'*), di mana pelaku tidak menghendaki akibat terlarang tersebut, namun akibat itu terjadi karena kecerobohan atau kelalaiannya (Oudah, 2007). Pembedaan antara kesengajaan dan kelalaian ini sangat penting karena akan menentukan berat ringannya sanksi yang dijatuhkan.

4. Penerapan Unsur Pidana pada Kasus Kejahatan Modern

Penerapan ketiga unsur ini pada kejahatan ekonomi digital memerlukan ketelitian. Misalnya, pada kasus *rug pull* dalam proyek DeFi:

a. Rukun Formal: Terpenuhi oleh undang-undang tentang penipuan.
b. Rukun Materiil: Perbuatannya adalah (1) membuat *smart contract* dan mengumpulkan dana investor, lalu (2) menarik semua likuiditas. Akibatnya adalah kerugian finansial total bagi investor. Kausalitasnya jelas.
c. Rukun Moril: Unsur kesengajaan (*niat jahat*) harus dibuktikan. Jaksa harus menunjukkan bahwa sejak awal pengembang tidak berniat membangun proyek yang sah, melainkan hanya ingin mengumpulkan dana lalu melarikan diri. Ini bisa dibuktikan dari jejak digital, komunikasi anonim, atau ketiadaan audit keamanan. Jika pengembang dapat membuktikan proyeknya gagal karena peretasan atau kesalahan kode yang tidak disengaja, maka unsur morilnya mungkin hanya kelalaian, bukan kesengajaan.

D. Konsep Harta (*Maal*) dan Kepemilikan dalam Islam

Karena fokus buku ini adalah kejahatan ekonomi, pemahaman yang benar tentang konsep "harta" (*māl*) dalam Islam menjadi sangat penting. Tidak semua hal yang bernilai dapat dianggap sebagai harta yang dilindungi oleh hukum pidana Islam. Sub-bab ini akan mendefinisikan kriteria harta, menegaskan prinsip perlindungan hak milik, dan yang terpenting, menganalisis status *cryptocurrency*—apakah ia dapat diklasifikasikan sebagai *māl* yang diakui syariah—sebuah pertanyaan kunci yang menentukan apakah pencuriannya dapat dihukum.

1. Definisi dan Kriteria Harta yang Diakui Syariah (Mutaqawwim)

Dalam fikih, *māl* (harta) secara umum didefinisikan sebagai segala sesuatu yang dapat dimiliki, disimpan, dan dimanfaatkan secara wajar (*'urf*), serta memiliki nilai ekonomi. Para yuris (khususnya mazhab Hanafi) membedakan antara *māl* secara umum dan *māl mutaqawwim*, yaitu harta yang nilainya diakui dan penggunaannya dibenarkan oleh syariah. Sesuatu dianggap *mutaqawwim* jika ia suci (*ṭāhir*) dan memiliki manfaat (*manfa'ah*) yang halal (Ibn Abidin, t.t.). Contoh harta yang tidak *mutaqawwim* (*ghair mutaqawwim*) bagi seorang Muslim adalah babi dan minuman keras; meskipun memiliki nilai pasar, kepemilikan dan pemanfaatannya dilarang oleh syariah.

2. Perlindungan Hak Milik (Hifzh al-Maal)

Perlindungan terhadap harta (*ḥifẓ al-māl*) adalah salah satu dari lima tujuan fundamental syariah (*Maqāshid al-Sharī'ah*). Syariah menetapkan serangkaian aturan yang sangat ketat untuk melindungi hak milik yang sah dari segala bentuk agresi. Ini termasuk larangan mencuri, merampok, menipu, korupsi, dan memakan riba. Sanksi pidana yang berat untuk kejahatan seperti pencurian (*sariqah*) dan perampokan (*ḥirābah*) menunjukkan betapa seriusnya Islam memandang perlindungan terhadap properti. Perlindungan ini adalah fondasi bagi stabilitas ekonomi dan keadilan sosial dalam masyarakat.

3. Larangan Memperoleh Harta Secara Batil

Prinsip utama dalam muamalah Islam adalah larangan memperoleh atau memakan harta orang lain dengan cara yang batil (*aklu amwāl al-nās*

bi al-bāṭil), sebagaimana ditegaskan dalam Al-Qur'an (An-Nisa: 29). "Batil" adalah istilah komprehensif yang mencakup segala cara perolehan yang tidak dibenarkan oleh syariah, seperti melalui paksaan, penipuan (*tadlīs*), perjudian (*maysir*), ketidakpastian yang ekstrem (*gharar*), dan riba. Prinsip ini menjadi landasan etis dan yuridis untuk melarang berbagai praktik dalam kejahatan ekonomi digital, seperti skema Ponzi, manipulasi pasar, dan penipuan investasi.

4. Analisis Status Cryptocurrency sebagai Harta dalam Fikih

Status fikih *cryptocurrency* sebagai *māl mutaqawwim* adalah subjek perdebatan kontemporer (*ijtihād*) di kalangan ulama.

a. Argumen yang Mendukung: Sebagian ulama berpendapat bahwa *cryptocurrency* memenuhi kriteria *māl* karena ia memiliki nilai ekonomi (dapat dipertukarkan dengan uang fiat), dapat disimpan (di *digital wallet*), dan dapat dialihkan kepemilikannya. Ia dianggap sebagai aset digital (*'urūḍ raqmiyyah*) yang statusnya mirip dengan hak kekayaan intelektual atau aset tidak berwujud lainnya yang diakui dalam fikih modern. Selama tidak digunakan untuk tujuan yang haram, ia dianggap *mutaqawwim* (Majelis Ulama Indonesia, 2021).

b. Argumen yang Menolak atau Berhati-hati: Sebagian ulama lain menyoroti sifat *gharar* (ketidakpastian ekstrem) karena volatilitasnya yang tinggi, potensi penggunaannya untuk aktivitas ilegal, dan ketiadaan otoritas penerbit yang jelas serta penjaminan fisik. Mereka berpendapat bahwa sifat spekulatifnya lebih mendekati perjudian (*maysir*) daripada investasi.

c. Posisi Dominan: Posisi yang paling banyak diterima adalah membedakan statusnya. Sebagai komoditas atau aset investasi, mayoritas lembaga fatwa (termasuk di Indonesia) memperbolehkannya dengan syarat-syarat tertentu. Namun, sebagai mata uang untuk alat tukar umum, banyak yang menolaknya karena tidak memenuhi syarat sebagai uang dalam Islam dan dapat mengganggu stabilitas moneter negara. Untuk tujuan buku ini, dengan mengacu pada fatwa MUI dan praktik legal di Indonesia, *cryptocurrency* dianggap sebagai aset digital yang memiliki nilai harta (*māliyyah*), sehingga pencurian atau perampasannya secara batil adalah sebuah kejahatan terhadap harta.

E. Asas Legalitas dalam Hukum Pidana Islam

Asas legalitas adalah pilar utama negara hukum modern. Sub-bab ini akan menunjukkan bahwa prinsip serupa telah lama berakar dalam hukum pidana Islam. Pembahasan akan berfokus pada adagium "tiada hukuman tanpa nash", namun juga akan menyoroti bagaimana prinsip ini tidak kaku, melainkan diimbangi oleh mekanisme fleksibilitas seperti *ijtihād* dan peran legislatif pemerintah dalam ranah *ta'zīr*. Implikasi dari dialektika antara kepastian hukum dan fleksibilitas ini terhadap penanggulangan kejahatan siber akan menjadi penutup sub-bab ini.

1. Prinsip "Tiada Hukuman Tanpa Nash" (La Jarimah wa la 'Uqubah illa bi Nash)

Prinsip ini adalah fondasi dari asas legalitas dalam hukum pidana Islam. Ia menegaskan bahwa suatu perbuatan tidak dapat dianggap sebagai tindak pidana (*jarīmah*) dan tidak dapat dikenai sanksi (*'uqūbah*) kecuali jika ada ketentuan hukum (*nash*) yang telah ada sebelumnya yang melarangnya. Prinsip ini digali dari beberapa ayat Al-Qur'an, di antaranya "Dan Kami tidak akan mengazab sebelum Kami mengutus seorang rasul" (Al-Isra: 15). Tujuannya adalah untuk menjamin keadilan, memberikan kepastian hukum, dan melindungi individu dari kesewenang-wenangan penguasa. Prinsip ini berlaku mutlak untuk kejahatan *hudūd* dan *qiṣāṣ* (Oudah, 2007).

2. Fleksibilitas melalui Ijtihad dan Qiyas dalam Kejahatan Baru

Kekakuan prinsip legalitas diimbangi oleh dinamisme metodologi hukum Islam. Untuk kasus-kasus baru yang tidak disebutkan secara eksplisit dalam *nash*, para yuris dapat menggunakan *ijtihād*, khususnya melalui *qiyās* (analogi). Jika sebuah kejahatan baru memiliki *'illah* (alasan hukum efektif) yang sama dengan kejahatan yang sudah ada hukumnya, maka hukum yang sama dapat diterapkan. Sebagai contoh, *'illah* dari larangan meminum *khamr* adalah karena memabukkan. Melalui *qiyās*, larangan ini dapat diperluas ke semua zat lain yang memabukkan, seperti narkotika, meskipun tidak secara eksplisit disebut dalam Al-Qur'an. Mekanisme ini memungkinkan hukum Islam untuk tetap relevan dalam menghadapi inovasi, termasuk dalam dunia kejahatan.

3. Peran Pemerintah (Ulil Amri) dalam Menetapkan Jarimah Ta'zir

Fleksibilitas terbesar terletak pada ranah *jarīmah ta'zīr*. Dalam kategori ini, asas legalitas dimaknai bahwa pemerintah atau otoritas legislatif (*ulil amri*) memiliki wewenang untuk membuat undang-undang (*qānūn* atau *taqnīn*) yang menetapkan perbuatan-perbuatan baru sebagai kejahatan dan menentukan sanksinya, demi tercapainya kemaslahatan umum. Legislasi ini dianggap sebagai bentuk *nash* modern yang mengikat warganya (Kamali, 2000). Selama undang-undang tersebut tidak bertentangan dengan prinsip-prinsip syariah yang lebih tinggi, ia sah dan wajib ditaati. Inilah mekanisme utama bagi negara Muslim modern untuk mengkriminalisasi perbuatan seperti kejahatan siber, pencucian uang, dan pelanggaran lalu lintas.

4. Implikasi Asas Legalitas pada Penanggulangan Kejahatan Siber

Implikasi dari konsep legalitas Islam ini terhadap kejahatan siber bersifat ganda. Di satu sisi, negara tidak bisa sewenang-wenang menghukum seorang peretas atau penipu digital tanpa adanya undang-undang yang jelas terlebih dahulu. Harus ada "nash" modern dalam bentuk UU ITE, UU TPPU, atau KUHP yang mendefinisikan perbuatan tersebut sebagai kejahatan. Di sisi lain, hukum Islam memberikan legitimasi penuh kepada negara untuk proaktif menciptakan undang-undang tersebut dalam kerangka *ta'zīr* untuk melindungi masyarakat dari bahaya (*mafsadah*) kejahatan siber. Dengan demikian, penegakan hukum terhadap kejahatan ekonomi digital oleh aparat negara berdasarkan undang-undang yang berlaku dapat dipandang sebagai implementasi dari kewenangan *ulil amri* untuk menetapkan *jarīmah ta'zīr* demi melindungi *ḥifẓ al-māl* dan ketertiban umum.

Analisis Mendalam Konsep Kunci Bab 2: Klasifikasi Jarimah (Hudud, Qisas-Diyat, Ta'zir)

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk memetakan seluruh spektrum tindak pidana dalam hukum Islam ke dalam tiga kategori yang berbeda secara fundamental. Klasifikasi ini bukan sekadar pengelompokan akademis, melainkan memiliki implikasi hukum yang sangat besar terkait:

1. Sumber Hukum: Dari mana sebuah perbuatan ditetapkan sebagai kejahatan?
2. Sifat Sanksi: Apakah hukumannya pasti dan tidak bisa diubah, atau fleksibel?
3. Hak yang Dilanggar: Apakah itu murni hak Allah (kepentingan publik), hak individu (korban), atau kombinasi keduanya?
4. Ruang Ijtihad: Sejauh mana pemerintah dan hakim memiliki kewenangan untuk berinovasi dan menyesuaikan hukum?

Pemahaman terhadap klasifikasi ini adalah pisau analisis utama untuk menentukan di mana posisi kejahatan-kejahatan modern seperti penipuan kripto, pencucian uang, dan peretasan.

Elemen-Elemen Kunci dalam Klasifikasi:

1. Kepastian Teks (*Nash*): Apakah jenis kejahatan dan sanksinya disebutkan secara eksplisit dan pasti dalam Al-Qur'an atau Hadis Mutawatir?
2. Hak yang Terkena Dampak: Siapa "korban" utamanya? Apakah masyarakat secara umum (hak Allah), atau individu tertentu (hak adami)?
3. Kewenangan Otoritas: Seberapa besar peran negara (ulil amr) dan hakim dalam mendefinisikan kejahatan dan menentukan sanksinya?

Analisis Komparatif: Tiga Kategori Jarimah

Tabel berikut membedah perbedaan fundamental antara *Hudud, Qisas-Diyat*, dan *Ta'zir*, yang menjadi inti dari Bab 2.

Fitur Kunci	Jarimah Hudud	Jarimah Qisas-Diyat	Jarimah Ta'zir (Konsep Kunci Utama)
Definisi	Kejahatan dengan sanksi yang telah ditetapkan secara pasti oleh *nash* untuk melindungi kepentingan publik.	Kejahatan terhadap jiwa dan badan (pembunuhan & penganiayaan) dengan sanksi retributif atau kompensasi.	Semua kejahatan lain yang jenis dan sanksinya ditentukan oleh kebijakan pemerintah (*ulil amr*) demi kemaslahatan.
Hak yang Dilanggar	Dominan Hak Allah (kepentingan publik). Pelanggaran terhadap tatanan dasar masyarakat.	Dominan Hak Individu/Adami (korban atau keluarga korban).	Hak Allah, Hak Individu, atau Keduanya. Sangat bervariasi tergantung jenis kejahatannya.
Sumber Hukum	Teks Primer (Al-Qur'an & Hadis). Jenis dan kadar sanksi bersifat pasti dan tidak bisa diubah.	Teks Primer. Jenis sanksi utama (*qisas*) pasti, namun ada alternatif (*diyat*, maaf) yang bergantung pada korban.	Ijtihad Pemerintah & Prinsip Umum Syariah. Didasarkan pada kebutuhan untuk mencegah kerusakan (*mafsadah*).
Sifat Sanksi	Tidak Fleksibel & Tidak Dapat Dimaafkan. Sanksi bersifat pasti (cth: potong tangan, cambuk).	Semi-Fleksibel. Korban/keluarga punya pilihan: menuntut balasan setimpal (*qisas*), menerima kompensasi finansial (*diyat*), atau memaafkan.	Sangat Fleksibel. Hakim memiliki diskresi luas: dari teguran, denda, penjara, publikasi, hingga hukuman mati.
Ruang Ijtihad	Sangat Sempit. Terbatas pada pembuktian yang sangat ketat. Tidak ada ijtihad pada jenis atau kadar hukuman.	Sempit. Terbatas pada pembuktian dan penentuan kadar *diyat* jika dipilih.	Sangat Luas. Pemerintah berijtihad untuk mendefinisikan kejahatan baru (membuat UU). Hakim berijtihad untuk menentukan sanksi yang paling tepat.
Relevansi dengan Kejahatan Kripto	Tidak Langsung Relevan. Kejahatan kripto tidak memenuhi syarat-syarat teknis dari 7 *jarimah hudud*.	Tidak Relevan. Tidak berkaitan langsung dengan kejahatan fisik terhadap jiwa/badan.	Sangat Relevan & Menjadi Satu-satunya Kerangka. Ini adalah kategori yang menampung semua bentuk kejahatan kripto (penipuan, pencucian uang, peretasan, dll.).

Kontribusi Konsep Klasifikasi dalam Bab 2:

Konsep ini adalah pilar teoretis dari keseluruhan buku. Tanpanya, analisis hukum pidana Islam akan berhenti.

1. Menyediakan "Pintu Masuk" Analisis: Dengan menunjukkan bahwa kejahatan kripto tidak masuk dalam kategori *Hudud* atau *Qisas*, Bab 2 secara logis mengarahkan seluruh analisis ke "pintu" *Jarimah Ta'zir*. Ini menyederhanakan masalah dan memberikan fokus yang jelas.
2. Memberikan Legitimasi pada Tindakan Negara: Konsep *Ta'zir* memberikan justifikasi syar'i bagi negara (pemerintah Indonesia) untuk membuat undang-undang (seperti UU ITE dan UU TPPU) guna menindak kejahatan digital. Tindakan legislasi ini dipandang sebagai pelaksanaan kewajiban *ulil amr* untuk menjaga ketertiban.
3. Menjadi Dasar bagi Bab-Bab Selanjutnya: Seluruh analisis di Bab 5 (Kualifikasi Kejahatan Kripto dalam Hukum Pidana Islam) dan Bab 9 (Analisis Kasus dari Perspektif Hukum Pidana Islam) sepenuhnya bergantung pada kerangka *Ta'zir* yang dibangun di Bab 2. Bab-bab tersebut pada dasarnya adalah aplikasi dari teori *Ta'zir* pada kasus-kasus konkret.

Secara esensial, Bab 2 menggunakan konsep klasifikasi *jarimah* untuk membangun sebuah "mesin analisis". Mesin ini menegaskan bahwa sementara teks-teks suci tidak menyebutkan "Bitcoin", prinsip-prinsip hukum Islam, melalui pintu *Ta'zir* yang dinamis, sepenuhnya mampu dan siap untuk menghadapi tantangan kejahatan di abad ke-21.

BAB 3

Tinjauan Fikih Muamalah terhadap Cryptocurrency

Setelah Bab 2 membangun fondasi teoretis hukum pidana Islam, Bab 3 melakukan langkah mundur yang esensial: menganalisis objek kejahatan itu sendiri—*cryptocurrency*—melalui kacamata hukum perdata Islam (*fiqh al-mu'āmalah*). Sebelum suatu tindakan terhadap sebuah objek dapat diklasifikasikan sebagai kejahatan (*jarīmah*), status hukum (*ḥukm*) dari objek dan transaksi yang melibatkannya harus ditetapkan terlebih dahulu. Dalam diskursus fikih kontemporer, perdebatan mengenai *cryptocurrency* adalah salah satu yang paling dinamis, membelah pandangan para ulama dan lembaga fatwa. *Research gap* yang diisi oleh bab ini adalah ketiadaan pembahasan terstruktur yang tidak hanya mengompilasi fatwa, tetapi juga secara analitis membedah *cryptocurrency* berdasarkan kategori-kategori fikih klasik (seperti *nuqūd* vs *sil'ah*) dan mengidentifikasi titik-titik rawan pelanggaran syariah (seperti *gharar*, *maysir*, dan *ribā*) dalam mekanisme spesifiknya. Pertanyaan penelitian utama bab ini adalah: Bagaimana status hukum *cryptocurrency* menurut *fiqh al-mu'āmalah*, dan pada titik mana saja dalam ekosistemnya terdapat potensi pelanggaran terhadap prinsip-prinsip transaksi syariah?

A. Cryptocurrency sebagai Alat Tukar (Nuqud)

Sub-bab ini secara khusus menguji kelayakan *cryptocurrency* untuk berfungsi sebagai "uang" (*nuqūd*) dari perspektif syariah. Analisis akan dimulai dengan mengidentifikasi syarat-syarat ideal sebuah mata uang dalam literatur ekonomi Islam, yang berfungsi sebagai tolok ukur. Kemudian, akan dipaparkan berbagai pandangan ulama global yang saling berhadapan mengenai isu ini, dengan fokus pada elemen-elemen problematis seperti *gharar* (ketidakpastian) dan *jahālah* (ketidaktahuan) yang melekat pada aset kripto. Pembahasan akan ditutup dengan penegasan status hukum *cryptocurrency* di Indonesia, yang secara tegas tidak diakui sebagai alat pembayaran yang sah, baik dari sisi hukum positif maupun fatwa keagamaan.

1. Syarat-syarat Uang dalam Perspektif Ekonomi Islam

Dalam pemikiran ekonomi Islam, fungsi utama uang adalah sebagai fasilitator transaksi, bukan sebagai komoditas yang dicari keuntungan darinya. Para yuris klasik seperti Imam Al-Ghazali dalam karyanya, *Ihya'*

Ulum al-Din, mengibaratkan uang seperti cermin yang hanya merefleksikan nilai barang lain tetapi tidak memiliki nilai intrinsik untuk dirinya sendiri. Berdasarkan pandangan ini dan ijtihad para ulama kontemporer, dapat disarikan beberapa syarat agar sesuatu dapat berfungsi sebagai uang. Syarat paling fundamental adalah penerimaan umum (*al-qabūl al-'āmm*), di mana masyarakat secara luas dan sukarela menerimanya sebagai medium pertukaran (Chapra, 2000). Tanpa penerimaan luas ini, sebuah entitas gagal memenuhi fungsi sosialnya sebagai uang.

Selain penerimaan umum, stabilitas nilai (*thabāt al-qīmah*) menjadi syarat krusial berikutnya. Uang harus dapat berfungsi sebagai penyimpan nilai (*store of value*) yang andal, sehingga masyarakat percaya bahwa daya belinya tidak akan tergerus secara drastis dalam waktu singkat. Syarat lainnya termasuk kemudahan untuk dibagi menjadi unit-unit yang lebih kecil (*divisibility*) untuk memfasilitasi transaksi kecil, serta adanya otoritas penerbit atau penjamin (*ḍamān*) yang kredibel. Dalam konteks negara modern, fungsi penjaminan ini diemban oleh bank sentral, yang bertanggung jawab menjaga stabilitas nilai mata uang dan kepercayaan publik terhadapnya.

2. Analisis Fatwa Ulama Global: Pro dan Kontra

Perdebatan mengenai status *cryptocurrency* sebagai uang telah mempolarisasi pandangan para ulama dan lembaga fatwa di seluruh dunia. Kelompok mayoritas, yang sering disebut sebagai kelompok kontra, menolak status *cryptocurrency* sebagai mata uang yang sah secara syariah. Lembaga-lembaga otoritatif seperti Dar al-Ifta di Mesir dan Direktorat Urusan Agama Turki (Diyanet) berargumen bahwa aset kripto gagal memenuhi syarat-syarat esensial uang. Mereka menyoroti ketiadaan otoritas pusat yang menjamin nilainya, volatilitas harga yang ekstrem yang menggagalkan fungsinya sebagai penyimpan nilai, serta kurangnya penerimaan umum yang meluas di tingkat global (Dar al-Ifta al-Misriyyah, 2018). Potensi penggunaannya untuk aktivitas ilegal seperti pencucian uang dan pendanaan terorisme juga menjadi pertimbangan utama dalam pendekatan *sadd al-żarā'i'* (menutup jalan menuju keburukan) yang mereka anut.

Di sisi lain, terdapat kelompok minoritas yang lebih akomodatif, yang berpendapat bahwa *cryptocurrency* dapat diterima sebagai bentuk uang konvensional (*'urfi money*). Mereka berargumen bahwa sejarah telah menunjukkan berbagai bentuk uang, dari kerang hingga kertas, yang nilainya juga didasarkan pada kesepakatan dan kepercayaan komunitas. Menurut pandangan ini, desentralisasi bukanlah kelemahan, melainkan sebuah fitur yang sejalan dengan semangat Islam untuk menghindari konsentrasi kekuasaan ekonomi. Selama suatu komunitas sepakat untuk menerima aset kripto sebagai alat tukar, maka ia dapat dianggap sah dalam lingkup komunitas tersebut (Pew Research Center, 2023). Pandangan ini sering kali menekankan pada potensi teknologi untuk inklusi keuangan, alih-alih hanya berfokus pada risikonya.

3. Isu Gharar (Ketidakpastian) dan Jahalah (Ketidaktahuan)

Dua konsep sentral dalam fikih muamalah yang menjadi penghalang utama bagi penerimaan *cryptocurrency* sebagai uang adalah *gharar* dan *jahālah*. *Gharar* didefinisikan sebagai ketidakpastian, ambiguitas, atau risiko yang berlebihan terkait dengan subjek atau hasil dari sebuah akad, yang berpotensi menimbulkan sengketa. Volatilitas harga *cryptocurrency* yang dapat berfluktuasi puluhan persen dalam sehari dipandang oleh banyak ulama sebagai bentuk *gharar fāḥish* (ketidakpastian yang parah). Seseorang yang menerima pembayaran dalam kripto tidak memiliki kepastian mengenai daya beli yang akan ia miliki beberapa jam kemudian, yang merusak fungsi uang sebagai pengukur nilai yang stabil (Al-Zuhaili, 2008).

Selain *gharar*, elemen *jahālah* (ketidaktahuan) juga sangat kental. Mayoritas pengguna dan bahkan sebagian pelaku pasar tidak sepenuhnya memahami kompleksitas teknologi *blockchain*, mekanisme konsensus, atau risiko keamanan siber yang melekat. Ketidaktahuan ini mencakup aspek fundamental seperti siapa yang sebenarnya mengendalikan jaringan, bagaimana sebuah koin diciptakan, dan apa yang terjadi jika terjadi serangan 51% atau kegagalan *smart contract*. Tingkat asimetri informasi yang tinggi ini menciptakan lingkungan di mana pihak yang lebih berpengetahuan dapat dengan mudah mengeksploitasi pihak yang kurang berpengetahuan, suatu kondisi yang sangat dihindari dalam etika transaksi Islam.

4. Status Hukum di Indonesia: Bukan Alat Pembayaran yang Sah

Di Indonesia, status hukum *cryptocurrency* sebagai alat pembayaran sangat jelas: dilarang. Sikap tegas ini diambil baik oleh otoritas moneter maupun otoritas keagamaan. Bank Indonesia, sebagai lembaga yang berwenang mengatur sistem pembayaran, secara konsisten menegaskan bahwa Rupiah adalah satu-satunya alat pembayaran yang sah di wilayah NKRI, sesuai dengan amanat Undang-Undang No. 7 Tahun 2011 tentang Mata Uang. Dalam berbagai siaran pers, BI menyatakan bahwa penggunaan aset kripto sebagai alat bayar berisiko mengancam stabilitas sistem keuangan dan kedaulatan moneter negara (Bank Indonesia, 2018).

Sikap pemerintah ini diperkuat oleh pandangan Majelis Ulama Indonesia (MUI). Dalam fatwanya, MUI secara eksplisit menyatakan bahwa penggunaan *cryptocurrency* sebagai mata uang hukumnya adalah haram. Alasan utama yang dikemukakan adalah karena ia mengandung unsur *gharar* (ketidakpastian), *dharar* (potensi bahaya dan kerusakan), dan tidak memenuhi syarat-syarat sebagai mata uang menurut syariah. Dengan adanya konvergensi antara pandangan regulator dan lembaga fatwa utama di Indonesia, tertutup sudah pintu bagi penggunaan *cryptocurrency* sebagai alat tukar yang sah di dalam negeri, sehingga setiap transaksi yang menggunakannya untuk tujuan pembayaran dapat dianggap tidak sesuai dengan hukum positif dan syariah.

B. Cryptocurrency sebagai Aset atau Komoditas (Sil'ah)

Jika ditolak sebagai uang, pintu lain yang dianalisis adalah status *cryptocurrency* sebagai aset atau komoditas (*sil'ah*) yang dapat diperjualbelikan. Sub-bab ini akan mengkaji bagaimana regulator Indonesia, khususnya Bappebti, memberikan landasan hukum bagi perdagangan aset kripto. Selanjutnya, akan dilakukan analisis dari perspektif fikih jual beli untuk menilai keabsahannya, sambil mengidentifikasi risiko utama berupa *maysir* (perjudian) yang sering kali menyertai praktik perdagangan spekulatif. Tinjauan terhadap fatwa MUI yang relevan akan memberikan pandangan penutup mengenai isu ini.

1. Pandangan BAPPEBTI: Cryptocurrency sebagai Aset Komoditi

Pemerintah Indonesia mengadopsi pendekatan dualistik yang pragmatis. Sementara Bank Indonesia melarangnya sebagai alat bayar, Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) justru memberikan ruang bagi aset kripto untuk eksis dalam ranah investasi. Melalui Peraturan Bappebti No. 5 Tahun 2019 dan pembaruan-pembaruannya, aset kripto secara resmi diakui sebagai komoditas yang dapat menjadi subjek kontrak berjangka dan diperdagangkan di bursa fisik aset kripto yang teregulasi. Langkah ini secara efektif memberikan legitimasi hukum bagi *cryptocurrency* sebagai objek investasi, setara dengan komoditas lain seperti emas, kopi, atau minyak sawit.

Dasar pertimbangan Bappebti adalah adanya permintaan pasar yang signifikan dari masyarakat Indonesia untuk berinvestasi pada aset kripto. Daripada membiarkannya berkembang di area abu-abu yang tidak teratur dan penuh risiko, pemerintah memilih untuk membawanya ke dalam kerangka regulasi. Tujuannya adalah untuk memberikan perlindungan kepada konsumen (investor), memastikan adanya transparansi transaksi, mencegah pencucian uang, dan tentunya, memperoleh potensi pendapatan negara dari pajak. Dengan demikian, dari sudut pandang hukum positif Indonesia, memperjualbelikan aset kripto di platform yang terdaftar di Bappebti adalah kegiatan yang legal.

2. Analisis Fikih tentang Jual Beli Aset Digital

Dari perspektif fikih, jual beli (*al-bay'*) aset digital dapat dianalisis dengan mengqiyaskannya (menganalogikan) pada jual beli hak (*ḥuqūq*) atau aset tidak berwujud (*intangible assets*), seperti hak cipta atau merek dagang, yang telah diterima dalam fikih kontemporer. Agar transaksi jual beli aset kripto dianggap sah, ia harus memenuhi rukun dan syarat jual beli. Rukunnya meliputi adanya para pihak (penjual dan pembeli), objek transaksi (*ma'qūd 'alaih*), dan ekspresi kesepakatan atau ijab kabul (*ṣīghah*). Syarat-syarat objeknya pun harus terpenuhi, yaitu objek tersebut harus ada, bernilai, dapat diidentifikasi dengan jelas, dimiliki sepenuhnya oleh penjual, dan dapat diserahterimakan (Ibn Qudamah, 1968).

Dalam transaksi jual beli Bitcoin, misalnya, rukun dan syarat ini secara teknis dapat terpenuhi. Objeknya jelas (misalnya, 0.5 BTC), ia dimiliki oleh penjual di dalam *wallet*-nya, dan dapat diserahterimakan secara digital dengan mentransfernya ke *wallet* pembeli. Selama aset kripto tersebut tidak memiliki *underlying* yang haram (misalnya, token yang merepresentasikan saham perusahaan judi), maka akad jual belinya pada dasarnya dapat dianggap sah. Namun, keabsahan akad ini belum tentu mencakup keabsahan motif atau cara perdagangannya, yang akan dibahas selanjutnya.

3. Isu Maysir (Perjudian) dalam Perdagangan Spekulatif

Meskipun akad jual belinya bisa sah, praktik perdagangan aset kripto sangat rentan terjerumus ke dalam larangan *maysir* (perjudian). *Maysir* didefinisikan sebagai setiap transaksi di mana perolehan harta bergantung sepenuhnya pada nasib atau kebetulan, bukan atas dasar produktivitas, kerja, atau analisis yang rasional. Batasan antara investasi yang halal (didasarkan pada riset fundamental terhadap nilai dan potensi sebuah proyek) dan spekulasi buta yang haram (mendekati *maysir*) menjadi sangat kabur dalam pasar aset kripto yang terkenal dengan volatilitas ekstrem dan minimnya informasi fundamental.

Praktik-praktik seperti *day trading* yang hanya mengandalkan fluktuasi harga jangka pendek, membeli koin hanya karena rumor atau *hype* di media sosial (*Fear of Missing Out*), atau berinvestasi pada *meme coins* yang secara terbuka tidak memiliki nilai guna, memiliki karakteristik yang sangat kuat dengan perjudian. Pelaku transaksi semacam ini tidak berniat memiliki aset untuk jangka panjang atau mendukung teknologinya, melainkan hanya bertaruh pada pergerakan harga. Inilah yang menjadi perhatian utama para ulama, karena Islam mendorong perolehan kekayaan melalui usaha produktif, bukan melalui permainan untung-untungan (Al-Qaradawi, 1999).

4. Fatwa MUI tentang Aset Kripto sebagai Komoditi

Menghadapi realitas ini, fatwa Majelis Ulama Indonesia (MUI) memberikan pandangan yang sangat berhati-hati dan bersyarat. Secara umum, fatwa tersebut menyatakan bahwa memperjualbelikan aset kripto yang bersifat spekulatif dan penuh ketidakpastian (*gharar*) hukumnya

adalah haram. MUI melihat bahwa mayoritas aset kripto yang ada saat ini tidak memiliki proyek dasar (*underlying asset*) yang riil dan pergerakan harganya murni didorong oleh spekulasi, sehingga lebih dekat ke *maysir* daripada investasi.

Namun, fatwa tersebut tidak menutup pintu sepenuhnya. Ia memberikan sebuah pengecualian penting: jika sebuah aset kripto memenuhi serangkaian syarat ketat, maka ia boleh diperjualbelikan. Syarat-syarat tersebut antara lain adalah (1) memiliki *underlying* dalam bentuk proyek riil atau aset yang dapat dinilai; (2) memiliki manfaat yang jelas dan tidak bertentangan dengan syariah; dan (3) memenuhi syarat sebagai *sil'ah* (komoditas) secara fikih, termasuk dapat diserahterimakan. Fatwa ini secara implisit mendorong munculnya aset kripto yang lebih bertanggung jawab, seperti token yang merepresentasikan kepemilikan properti, sukuk digital, atau komoditas fisik, sambil memberikan lampu merah bagi aset kripto yang murni spekulatif.

C. Unsur Riba dalam Transaksi Cryptocurrency

Setelah membahas isu *gharar* dan *maysir*, analisis beralih ke salah satu larangan paling fundamental dalam keuangan Islam: *ribā*. Ekosistem *cryptocurrency* yang inovatif telah melahirkan berbagai produk keuangan baru yang menjanjikan imbal hasil bagi pemilik aset. Sub-bab ini akan mengidentifikasi potensi jebakan *ribā* dalam mekanisme-mekanisme tersebut. Setelah mendefinisikan konsep *ribā* dan jenis-jenisnya, analisis akan difokuskan pada praktik modern seperti *staking* dan *lending* yang ditawarkan oleh banyak platform, termasuk dalam ranah Keuangan Terdesentralisasi (DeFi), dan diakhiri dengan eksplorasi upaya untuk menciptakan alternatif yang sesuai syariah.

1. Konsep Riba dan Jenis-jenisnya (Nasi'ah dan Fadhl)

Ribā adalah konsep sentral dalam hukum keuangan Islam, yang secara tegas diharamkan dalam Al-Qur'an. Secara bahasa, *ribā* berarti "tambahan" atau "pertumbuhan". Dalam terminologi fikih, ia merujuk pada setiap kelebihan atau tambahan yang disyaratkan dalam transaksi tertentu tanpa adanya padanan (*'iwad*) yang dibenarkan oleh syariah. Larangan ini

bertujuan untuk mencegah eksploitasi, mendorong pembiayaan berbasis aset riil, dan menegakkan keadilan dalam transaksi utang-piutang.

Para ulama membagi *ribā* menjadi dua kategori utama. Pertama adalah Ribā Nasi'ah, yang juga dikenal sebagai *ribā al-jahiliyyah*. Ini adalah jenis *ribā* yang paling umum, yaitu bunga yang dikenakan atas pinjaman berdasarkan berjalannya waktu. Contohnya adalah meminjamkan 100 dan mensyaratkan pengembalian sebesar 110 setelah satu tahun. Kedua adalah Ribā Fadhl, yaitu pertukaran barang-barang ribawi (seperti emas, perak, gandum, kurma) yang sejenis dengan takaran atau kualitas yang berbeda secara tunai. Tujuannya adalah untuk menutup celah yang dapat mengarah pada *ribā nasi'ah* (Saeed, 2016).

2. Analisis Potensi Riba dalam Staking dan Lending Crypto

Banyak platform aset kripto menawarkan produk yang secara fungsional sangat mirip dengan produk perbankan konvensional, sehingga memicu analisis mengenai potensi *ribā*. Salah satu yang paling umum adalah *crypto lending*. Dalam skema ini, pengguna "mendepositokan" atau meminjamkan aset kriptonya ke sebuah platform dan dijanjikan imbal hasil tetap, misalnya 5% per tahun (APY). Platform kemudian meminjamkan dana tersebut kepada pihak lain dengan bunga yang lebih tinggi. Dari perspektif fikih, skema ini adalah contoh textbook dari *qarḍ jarra naf'an* (pinjaman yang menghasilkan keuntungan bagi pemberi pinjaman), yang merupakan esensi dari *ribā nasi'ah*.

Praktik lain yang populer adalah *staking*, khususnya pada *blockchain* yang menggunakan mekanisme konsensus *Proof-of-Stake* (PoS). Di sini, pengguna "mengunci" sejumlah koinnya untuk membantu mengamankan jaringan dan memvalidasi transaksi, dan sebagai imbalannya, mereka menerima koin baru sebagai *reward*. Status fikih *staking* lebih menjadi perdebatan. Sebagian ulama memandangnya sebagai bentuk upah (*ujrah*) atas jasa menjaga keamanan jaringan, sehingga diperbolehkan. Namun, pandangan lain yang lebih kritis melihatnya sebagai skema di mana "uang menghasilkan uang" tanpa adanya aktivitas ekonomi riil. Jika imbalan *staking* dilihat murni sebagai hasil dari mengunci aset (mirip bunga deposito), maka ia dapat dikategorikan mendekati *ribā* (El-Gamal, 2006).

3. Skema Pinjaman Berbasis Bunga dalam Platform DeFi

Keuangan Terdesentralisasi (DeFi) sering kali disebut sebagai revolusi keuangan, namun banyak dari protokolnya yang paling populer pada dasarnya mereplikasi model perbankan konvensional berbasis bunga di atas *blockchain*. Platform *lending* DeFi seperti Aave, Compound, atau MakerDAO beroperasi sebagai pasar uang algoritmik. Pengguna dapat menyetorkan aset kripto mereka ke dalam sebuah *liquidity pool* dan langsung mendapatkan bunga secara *real-time*. Di sisi lain, peminjam dapat mengambil pinjaman dari *pool* ini dengan memberikan agunan (*collateral*) dan membayar tingkat bunga yang ditentukan oleh algoritma berdasarkan penawaran dan permintaan.

Meskipun prosesnya otomatis melalui *smart contract* dan tidak ada bank sebagai perantara, model bisnis fundamentalnya tetaplah intermediasi kredit berbasis bunga. Penyedia likuiditas (pemberi pinjaman) menerima tambahan (*ribā*) atas dana yang mereka setorkan, dan peminjam membayar tambahan tersebut. Fakta bahwa prosesnya terdesentralisasi tidak mengubah esensi akadnya, yang dari perspektif hukum Islam tetap merupakan transaksi ribawi (Schär, 2021). Hal ini menunjukkan bahwa inovasi teknologi tidak serta-merta mengubah status hukum sebuah transaksi jika substansi ekonominya tetap sama.

4. Upaya Menghindari Riba dalam Ekosistem Kripto

Merespons kekhawatiran akan *ribā*, komunitas Muslim global mulai mengembangkan proyek-proyek "DeFi Syariah" atau *Islamic DeFi*. Inisiatif-inisiatif ini bertujuan untuk mereplikasi fungsionalitas DeFi namun dengan menggunakan akad-akad yang sesuai syariah. Alih-alih pinjaman berbasis bunga, platform ini mencoba mengimplementasikan skema bagi hasil seperti *muḍārabah* (kemitraan investasi di mana satu pihak memberikan modal dan pihak lain mengelola) atau *mushārakah* (kemitraan di mana semua pihak menyumbang modal dan kerja).

Sebagai contoh, sebuah *liquidity pool* dapat dirancang berdasarkan akad *mushārakah*, di mana dana yang terkumpul diinvestasikan pada proyek-proyek produktif yang halal, dan keuntungannya dibagikan kepada para penyedia likuiditas sesuai nisbah yang disepakati. Tantangannya tentu sangat besar, terutama dalam hal memastikan investasi dilakukan pada

sektor riil dan melakukan audit kepatuhan syariah secara transparan di lingkungan *on-chain*. Meskipun masih dalam tahap awal dan menghadapi banyak kendala teknis dan hukum, upaya ini menunjukkan adanya jalan untuk memanfaatkan teknologi *blockchain* sejalan dengan prinsip keuangan Islam.

D. Prinsip Transparansi dan Keadilan

Prinsip keterbukaan (*disclosure*), transparansi, dan keadilan merupakan fondasi dari etika transaksi dalam Islam. Sub-bab ini akan menganalisis bagaimana fitur-fitur inheren dalam teknologi *cryptocurrency*, terutama anonimitas dan pseudonimitas, dapat berbenturan dengan prinsip-prinsip luhur ini. Akan dibahas pula bagaimana lingkungan ini menjadi subur bagi praktik-praktik terlarang seperti *tadlīs* (penipuan informasi) dan *ghabn* (kecurangan harga), serta diakhiri dengan penegasan mengenai pentingnya peran etika Islam dalam membangun ekosistem digital yang dapat dipercaya.

1. Sifat Anonim dan Pseudonim dalam Transaksi Kripto

Salah satu narasi utama yang mempopulerkan *cryptocurrency* adalah kemampuannya untuk memberikan privasi finansial. Namun, privasi ini sering kali berwujud pseudonimitas atau bahkan anonimitas penuh, yang menimbulkan tantangan etis dan hukum. Pada *blockchain* seperti Bitcoin, transaksi bersifat pseudonim; alamat dompet dapat dilihat oleh publik, namun identitas pemiliknya di dunia nyata tidak terikat secara langsung ke alamat tersebut. Ini menciptakan selubung kerahasiaan yang dapat dimanfaatkan untuk tujuan ilegal, seperti menyembunyikan hasil korupsi atau melakukan transaksi di pasar gelap.

Tingkat kerahasiaan ini semakin dalam pada *privacy coins* seperti Monero atau Zcash, yang menggunakan teknologi kriptografi canggih untuk menyembunyikan alamat pengirim, penerima, dan jumlah transaksi. Meskipun privasi adalah hak yang dihargai, anonimitas absolut bertentangan dengan prinsip transparansi dalam Islam, yang menuntut kejelasan pihak-pihak yang bertransaksi (*ma'rifat al-'āqidain*) untuk memastikan akuntabilitas dan mencegah kezaliman. Lingkungan yang anonim menyulitkan penegakan hukum, penyelesaian sengketa, dan penelusuran dana jika terjadi penipuan.

2. Potensi Tadlis (Penipuan Informasi) dan Ghabn (Kecurangan Harga)

Lingkungan yang minim regulasi dan penuh dengan asimetri informasi seperti pasar kripto adalah lahan subur bagi praktik *tadlīs* dan *ghabn*. *Tadlīs* adalah tindakan penipuan di mana penjual secara sengaja menyembunyikan cacat barang atau memberikan informasi yang salah untuk memperdaya pembeli. Dalam dunia kripto, ini terwujud dalam berbagai bentuk: *whitepaper* proyek yang menjanjikan teknologi revolusioner padahal hanya salinan dari proyek lain, klaim kemitraan palsu dengan perusahaan besar, atau promosi oleh *influencer* yang dibayar tanpa mengungkapkannya kepada publik.

Ghabn adalah ketidakseimbangan atau kecurangan harga yang signifikan, di mana satu pihak mengeksploitasi ketidaktahuan pihak lain. Skema *pump and dump* adalah contoh sempurna dari gabungan *tadlīs* dan *ghabn fāḥish* (kecurangan harga yang ekstrem). Sekelompok manipulator (sering kali anonim) menyebarkan informasi positif palsu (*tadlīs*) untuk menaikkan harga sebuah koin secara artifisial (*pump*), lalu menjual semua aset mereka di puncak harga kepada investor ritel yang terlambat masuk karena FOMO. Akibatnya, harga anjlok dan investor ritel menderita kerugian besar, sebuah bentuk memakan harta orang lain secara batil.

3. Pentingnya Keterbukaan (Disclosure) dalam Proyek Kripto

Untuk memerangi praktik-praktik curang ini, penerapan prinsip keterbukaan (*disclosure*) menjadi sebuah keharusan etis dan praktis. Sebuah proyek *cryptocurrency* yang dikembangkan dengan niat baik seharusnya tidak bersembunyi di balik anonimitas. Keterbukaan ini mencakup beberapa aspek. Pertama, identitas tim pengembang harus jelas dan dapat diverifikasi (*doxxed team*), sehingga ada pihak yang dapat dimintai pertanggungjawaban. Kedua, dokumentasi proyek (*whitepaper*) harus realistis, jujur mengenai tantangan, dan tidak membuat janji yang berlebihan.

Ketiga, alokasi token (*tokenomics*) harus transparan, menunjukkan berapa persen token yang dipegang oleh tim, investor awal, dan yang dialokasikan untuk komunitas. Ini penting untuk mendeteksi potensi *rug pull* atau tekanan jual yang besar dari tim. Keempat, dan yang terpenting,

smart contract yang menjadi inti dari proyek harus diaudit oleh lembaga audit keamanan pihak ketiga yang memiliki reputasi baik. Hasil audit ini harus dipublikasikan secara penuh, termasuk temuan kerentanan dan langkah-langkah perbaikannya. Tanpa standar keterbukaan seperti ini, sulit untuk membedakan antara proyek yang sah dan skema penipuan.

4. Peran Etika Islam dalam Membangun Kepercayaan

Pada akhirnya, dalam lingkungan yang terdesentralisasi dan sering kali berada di luar jangkauan regulasi tradisional, etika menjadi garda pertahanan yang paling fundamental. Prinsip-prinsip etika bisnis Islam (*akhlāq*) menawarkan kerangka kerja yang kokoh untuk membangun ekosistem yang adil dan dapat dipercaya. Prinsip-prinsip seperti kejujuran (*ṣidq*) dalam komunikasi, memegang amanah (*amānah*) atas dana investor, bersikap adil (*'adl*) kepada semua pemangku kepentingan, dan melakukan pekerjaan dengan profesionalisme dan kesempurnaan (*itqān*) harus menjadi landasan bagi setiap pengembang dan pelaku pasar.

Membangun proyek kripto bukan hanya tentang menulis kode, tetapi juga tentang membangun komunitas dan kepercayaan. Seorang pengembang Muslim, misalnya, memiliki tanggung jawab etis untuk memastikan produknya tidak memfasilitasi *gharar*, *maysir*, atau *ribā*. Ia juga harus transparan mengenai risiko dan tidak menggunakan taktik pemasaran yang menipu. Dengan menginternalisasi nilai-nilai etis ini, komunitas dapat secara proaktif melakukan swa-regulasi dan menciptakan standar yang lebih tinggi, sehingga membangun ekosistem digital yang tidak hanya inovatif secara teknologi tetapi juga sehat secara moral.

E. Pandangan Komparatif Lembaga Fatwa di Dunia

Status fikih *cryptocurrency* adalah isu ijtihad kontemporer, sehingga tidak mengherankan jika terdapat perbedaan pandangan di antara para ulama dan lembaga fatwa di seluruh dunia. Sub-bab ini menyajikan analisis komparatif dari beberapa fatwa dan pandangan yang paling berpengaruh. Dengan membandingkan posisi dari Timur Tengah, Asia Tenggara, dan konteks lainnya, kita dapat memahami perbedaan metodologi dan prioritas yang mendasari kesimpulan mereka. Analisis ini akan diakhiri dengan sebuah sintesis yang relevan untuk diterapkan dalam konteks spesifik Indonesia.

1. Fatwa dari Mesir, Arab Saudi, dan Turki

Lembaga-lembaga fatwa terkemuka di Timur Tengah umumnya mengambil sikap yang sangat konservatif dan cenderung melarang. Dar al-Ifta Mesir, salah satu lembaga fatwa paling berpengaruh di dunia Sunni, mengeluarkan fatwa pada tahun 2018 yang mengharamkan perdagangan Bitcoin. Alasan utamanya adalah tingkat *gharar* yang tinggi akibat volatilitas ekstrem, potensi penggunaannya untuk pencucian uang dan pendanaan terorisme karena sifat anonimnya, serta ketiadaan penjamin atau regulator pusat. Sikap serupa, meskipun tidak dalam bentuk fatwa formal, juga ditunjukkan oleh ulama senior di Arab Saudi yang memperingatkan masyarakat tentang bahaya spekulasi dan penipuan di pasar kripto.

Di Turki, Direktorat Urusan Agama (Diyanet) juga menyatakan bahwa perdagangan aset kripto pada saat ini tidak sejalan dengan ajaran Islam. Mereka menyoroti sifatnya yang sangat spekulatif, ketiadaan pengawasan oleh otoritas, dan potensinya untuk memperkaya sebagian kecil orang secara tidak adil dengan merugikan banyak orang lain. Pandangan dari ketiga negara ini secara umum mencerminkan pendekatan *sadd al-żarā'i'* (tindakan preventif), di mana potensi kerusakan (*mafsadah*) dari teknologi ini dipandang jauh lebih besar daripada potensi manfaatnya (*maṣlaḥah*).

2. Pandangan dari Lembaga Fikih di Malaysia dan negara lainnya

Berbeda dengan Timur Tengah, pendekatan di Asia Tenggara, khususnya Malaysia, menunjukkan pragmatisme yang lebih besar. Dewan Penasihat Syariah dari Komisi Sekuritas Malaysia (SAC-SC), dalam sebuah resolusi penting pada tahun 2020, memutuskan bahwa investasi dan perdagangan aset digital adalah diperbolehkan (harus), dengan syarat ia dilakukan melalui bursa yang terdaftar dan diatur secara resmi oleh Komisi Sekuritas. Pendekatan Malaysia tidak mengharamkan teknologi itu sendiri, melainkan fokus pada pentingnya regulasi untuk memitigasi risiko. Mereka memandang aset digital sebagai realitas ekonomi baru yang harus dikelola, bukan dihindari.

Di luar lembaga resmi, banyak cendekiawan Muslim individual di Barat dan Asia yang juga mengambil sikap yang lebih bernuansa. Mereka sering kali membedakan antara teknologi *blockchain* (yang dipandang netral dan bermanfaat) dan aset kripto spesifik (yang harus dinilai kasus per kasus).

Mereka berpendapat bahwa jika sebuah aset kripto memiliki nilai guna yang jelas, didukung oleh proyek yang produktif, dan tidak digunakan untuk tujuan haram, maka ia dapat dianggap sebagai harta (*māl*) yang sah untuk dimiliki dan diperdagangkan.

3. Analisis Perbedaan Metodologi dan Pertimbangan

Perbedaan pandangan yang tajam ini dapat ditelusuri ke perbedaan dalam metodologi hukum (*manhaj al-istinbāṭ*) dan prioritas. Lembaga yang melarang (Mesir, Turki) cenderung memberikan bobot yang lebih besar pada dalil-dalil umum tentang larangan *gharar*, *maysir*, dan kewajiban untuk melindungi harta. Mereka menerapkan prinsip kehati-hatian (*iḥtiyāṭ*) dan *sadd al-żarā'i'* secara ketat, dengan asumsi bahwa tanpa regulasi yang kuat, teknologi ini lebih banyak membawa keburukan.

Sebaliknya, lembaga yang memperbolehkan dengan syarat (Malaysia) menerapkan kaidah fikih "*al-aṣl fī al-mu'āmalāt al-ibāḥah*" (hukum asal dalam transaksi adalah kebolehan) selama tidak ada dalil yang secara tegas melarangnya. Mereka fokus pada bagaimana menciptakan kemaslahatan (*maṣlaḥah*) melalui regulasi yang efektif. Pendekatan ini lebih akomodatif terhadap inovasi dan adat kebiasaan baru (*'urf jadīd*), dengan keyakinan bahwa risiko dapat dikelola. Perbedaan konteks—di mana Malaysia sudah memiliki kerangka regulasi bursa kripto yang berfungsi—juga memainkan peran krusial dalam membentuk pandangan mereka.

4. Sintesis Pandangan untuk Konteks Indonesia

Konteks Indonesia, dengan dualisme regulasi (BI melarang, Bappebti mengatur) dan fatwa MUI yang bersyarat, tampaknya merupakan sintesis dari berbagai pandangan global ini. Fatwa MUI yang mengharamkan kripto sebagai mata uang sejalan dengan pandangan konservatif dari Mesir dan Turki, serta sejalan dengan kebijakan Bank Indonesia. Ini adalah penerapan prinsip *sadd al-żarā'i'* untuk melindungi kedaulatan moneter dan stabilitas keuangan.

Namun, fatwa yang sama yang membuka kemungkinan memperbolehkan kripto sebagai aset komoditas dengan syarat ketat (memiliki *underlying*, manfaat jelas, dll.) mencerminkan pendekatan pragmatis seperti yang terlihat di Malaysia. Ini adalah upaya untuk menerapkan kaidah "*al-ibāḥah*"

dalam ranah investasi, sambil menetapkan pagar-pagar syariah yang jelas. Pendekatan hibrida ini, meskipun mungkin terlihat kompleks, sebenarnya sangat kontekstual. Ia mengakui realitas adanya pasar aset kripto yang diatur oleh Bappebti, sambil tetap memberikan panduan moral dan etis yang ketat kepada umat Islam untuk membedakan antara investasi yang sah dan spekulasi yang haram.

Analisis Mendalam Konsep Kunci Bab 3: Dualisme Status Fikih Cryptocurrency (Nuqud vs. Sil'ah)

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk membedah dan memetakan perdebatan sentral di kalangan ulama dan lembaga fatwa mengenai hakikat (*takyif fiqhi*) dari *cryptocurrency*. Bab 3 menggunakan dualisme ini untuk menunjukkan bahwa tidak ada jawaban tunggal yang sederhana. Status sebuah *cryptocurrency* akan sangat bergantung pada karakteristik, fungsi, dan bagaimana ia diperlakukan di pasar.

Pemahaman terhadap dualisme ini krusial karena:

1. Menentukan Aturan Main: Jika dianggap sebagai uang (nuqud), maka ia tunduk pada aturan ketat tentang riba dan pertukaran mata uang (*bay' al-sarf*).
2. Membuka Pintu Transaksi: Jika dianggap sebagai aset/komoditas (*sil'ah*), maka ia pada dasarnya boleh diperjualbelikan (*bay'*) selama terhindar dari unsur *gharar* (ketidakpastian) dan *maysir* (perjudian).

   Menjelaskan Perbedaan Fatwa: Dualisme ini adalah alasan utama mengapa fatwa-fatwa di seluruh dunia bisa berbeda. Sebagian ulama fokus pada fungsinya yang mirip uang, sementara yang lain (termasuk regulator Indonesia) fokus pada sifatnya sebagai aset digital yang diperdagangkan.

Elemen-Elemen Kunci dalam Penentuan Status:

a. Standar Penerimaan Umum (*'Urf*): Apakah ia diterima secara luas oleh masyarakat sebagai alat tukar?
b. Stabilitas Nilai (*Thabat*): Apakah nilainya relatif stabil sehingga bisa menjadi penyimpan nilai yang andal?
c. Jaminan Otoritas (*I'tibar al-Sultah*): Apakah ia diakui dan dijamin oleh otoritas/pemerintah yang sah?
d. Kejelasan Fisik/Konseptual (*Ma'lum*): Apakah wujud dan mekanismenya jelas dan tidak mengandung ketidakpastian yang berlebihan (*gharar*)?

Analisis Komparatif: Cryptocurrency sebagai Uang vs. sebagai Aset/ Komoditas

Tabel berikut membedah implikasi dari masing-masing status fikih terhadap *cryptocurrency*.

Fitur Kunci	Jika Dianggap Uang (Nuqud)	Jika Dianggap Aset/Komoditas (Sil'ah)
Dasar Argumentasi	Fokus pada fungsi potensialnya sebagai alat tukar (*medium of exchange*) dan satuan hitung (*unit of account*). Namanya "currency".	Fokus pada **sifat** dasarnya sebagai kode digital yang memiliki nilai pasar, diperjualbelikan untuk mencari keuntungan.
Aturan Fikih Utama	Hukum Pertukaran Mata Uang (*Bay' al-Sarf*): Harus dilakukan secara tunai/spot (*taqabud*), tidak boleh ditunda. Pertukaran sejenis (BTC ke BTC) harus sama nilainya untuk menghindari Riba Fadhl.	Hukum Jual Beli (*Al-Bay'*): Pada dasarnya boleh (*mubah*), selama memenuhi rukun dan syarat jual beli.
Isu Kritis Utama	Gharar & Jahalah: Volatilitasnya yang ekstrem membuatnya gagal sebagai penyimpan nilai yang andal. Tidak ada jaminan otoritas (*ghairu mu'tabar*).	Maysir (Perjudian): Perdagangan yang murni spekulatif tanpa analisis fundamental dianggap mendekati perjudian. Gharar: Banyak proyek kripto tidak memiliki kegunaan nyata (*underlying asset*) yang jelas.
Implikasi pada Staking/Lending	Sangat berisiko Riba Nasi'ah. Meminjamkan "uang" (kripto) dan mendapatkan imbalan "bunga" (kripto tambahan) adalah skema riba yang jelas.	Dapat dianalogikan dengan sewa-menyewa aset (*ijarah*) atau bagi hasil (*mudharabah*), JIKA imbalan yang didapat berasal dari aktivitas ekonomi riil (misal: biaya validasi transaksi), bukan sekadar bunga pinjaman.
Pandangan Lembaga	Cenderung Melarang/Haram. Diadopsi oleh banyak lembaga fatwa di Timur Tengah (seperti Mesir) dan menjadi dasar Fatwa MUI yang mengharamkan kripto sebagai mata uang.	Cenderung Membolehkan dengan Syarat Ketat. Diadopsi oleh BAPPEBTI di Indonesia dan Shariah Advisory Council di Malaysia. Menjadi dasar Fatwa MUI yang membolehkan kripto sebagai aset/komoditi jika memenuhi syarat.
Kesimpulan Status	GAGAL memenuhi syarat sebagai uang dalam fikih Islam karena volatilitas ekstrem, kurangnya penerimaan umum, dan ketiadaan jaminan otoritas.	DAPAT DITERIMA sebagai aset digital yang diperdagangkan, NAMUN harus bersih dari unsur *gharar*, *maysir*, dan *riba*, serta memiliki kegunaan (*manfa'ah*) yang jelas.

Kontribusi Konsep Dualisme dalam Bab 3:

Konsep ini adalah mesin analisis fikih muamalah dalam buku ini.

1. Menjelaskan Kebingungan Publik: Dengan memetakan dualisme ini, Bab 3 menjelaskan kepada pembaca mengapa ada begitu banyak pendapat yang simpang siur mengenai hukum *cryptocurrency*. Ini bukan sekadar "halal vs. haram", melainkan "halal/haram sebagai apa?".
2. Memberikan Landasan bagi Analisis Kejahatan: Pemahaman ini krusial untuk Bab 4 dan 5. Misalnya, penipuan investasi kripto (skema Ponzi) dapat dianalisis sebagai bentuk jual beli aset yang mengandung *gharar* dan *tadlis* (penipuan) yang ekstrem. Transaksi *lending* di platform DeFi dapat dianalisis sebagai praktik riba yang dilarang.
3. Menjembatani Fikih dan Hukum Positif: Konsep ini menunjukkan adanya titik temu antara pandangan fikih mayoritas dengan hukum positif di Indonesia. Keputusan BAPPEBTI untuk mengklasifikasikan kripto sebagai komoditas (bukan alat pembayaran) ternyata sangat sejalan dengan kesimpulan fikih bahwa kripto lebih cocok diperlakukan sebagai *sil'ah* (aset/komoditas) daripada *nuqud* (uang).

Secara ringkas, Bab 3 menggunakan dualisme *Nuqud vs. Sil'ah* untuk membedah DNA *cryptocurrency* dari sudut pandang hukum ekonomi Islam. Hasil bedah ini menyimpulkan bahwa *cryptocurrency* bukanlah uang yang sah secara syar'i, melainkan sebuah aset digital yang hukumnya bergantung pada bagaimana ia diciptakan, diperdagangkan, dan dimanfaatkan. Kesimpulan inilah yang membuka jalan bagi analisis kejahatan yang lebih mendalam di bab-bab berikutnya.

BAB 4

Modus Operandi Kejahatan Ekonomi Digital Menggunakan Cryptocurrency

Setelah Bab 3 menetapkan status hukum *cryptocurrency* dalam ranah *mu'āmalah*, Bab 4 beralih ke manifestasi konkret dari sisi gelapnya: modus operandi kejahatan. Pemahaman mendalam mengenai "bagaimana" kejahatan ini dilakukan adalah prasyarat esensial sebelum merumuskan "bagaimana" hukum dapat meresponsnya. Dalam diskursus kriminologi digital, evolusi modus operandi kejahatan sering kali lebih cepat daripada evolusi kerangka hukum. *Research gap* yang hendak diisi oleh bab ini adalah kurangnya pembahasan sistematis dalam literatur berbahasa Indonesia yang mengkategorikan dan menjelaskan secara teknis berbagai modus operandi kejahatan berbasis *cryptocurrency*, dari penipuan sederhana hingga operasi pencucian uang yang kompleks. Pertanyaan penelitian utama yang memandu bab ini adalah: Bagaimana karakteristik teknologi *cryptocurrency* dan ekosistemnya dimanfaatkan oleh para pelaku kriminal untuk menjalankan berbagai jenis kejahatan ekonomi digital, dan apa saja pola umum yang dapat diidentifikasi dari modus operandi tersebut?

A. Penipuan (*Scam*) dan Investasi Bodong

Penipuan dan investasi bodong merupakan bentuk kejahatan ekonomi digital yang paling umum dan merugikan masyarakat luas. Sifat pasar kripto yang spekulatif, ditambah dengan rendahnya literasi keuangan digital, menciptakan lingkungan yang ideal bagi para penipu. Sub-bab ini akan membedah berbagai modus operandi penipuan yang paling sering terjadi, mulai dari skema Ponzi klasik yang dikemas ulang, proyek-proyek fiktif yang dirancang untuk menipu investor, hingga teknik rekayasa sosial seperti *phishing* untuk mencuri aset secara langsung.

1. Skema Ponzi dan Piramida Berkedok Investasi Kripto

Skema Ponzi adalah modus penipuan investasi klasik di mana keuntungan bagi investor awal dibayarkan menggunakan dana dari investor yang lebih baru, bukan dari keuntungan usaha yang sah. Dalam dunia kripto, skema ini sering kali dikemas dalam bentuk platform "investasi" atau "penambangan awan" (*cloud mining*) yang menjanjikan imbal hasil harian atau bulanan yang sangat tinggi dan tidak realistis (misalnya, 1-5% per hari). Para pelaku memanfaatkan euforia pasar dan jargon-jargon

teknis untuk meyakinkan korban bahwa keuntungan fantastis tersebut dimungkinkan oleh "robot trading canggih" atau "operasi penambangan skala besar". Skema ini akan terus berjalan selama ada aliran dana baru yang masuk untuk membayar investor lama.

Serupa dengan Ponzi, skema piramida juga marak terjadi. Dalam skema ini, peserta diwajibkan untuk merekrut anggota baru untuk mendapatkan komisi, dengan produk investasi kripto hanya sebagai kedok. Fokus utamanya adalah pada perekrutan, bukan pada nilai atau kegunaan produk itu sendiri. Kedua skema ini pada akhirnya pasti akan runtuh ketika tidak ada lagi investor baru yang dapat direkrut, menyebabkan kerugian total bagi mayoritas peserta yang bergabung belakangan. Sifat transaksi kripto yang lintas batas dan sulit dilacak membuat para operator skema ini dapat dengan mudah melarikan diri dengan dana korban tanpa jejak.

Penggunaan *cryptocurrency* dalam skema ini memberikan beberapa keuntungan bagi penipu. Pertama, mereka dapat menjangkau audiens global dengan mudah melalui media sosial dan platform pesan instan. Kedua, transfer dana dalam bentuk kripto bersifat instan dan tidak dapat dibatalkan (*irreversible*), tidak seperti transfer bank yang masih bisa dilacak atau dibekukan. Ketiga, dengan menggunakan alamat dompet anonim, identitas asli para penipu tetap tersembunyi, mempersulit upaya penegakan hukum untuk menuntut pertanggungjawaban mereka setelah skema tersebut runtuh.

2. Penawaran Koin Palsu (*Shitcoins*) dan Proyek Fiktif (*Rug Pull*)

Salah satu modus penipuan yang paling merajalela di era DeFi adalah *rug pull*. Istilah ini merujuk pada situasi di mana tim pengembang sebuah proyek *cryptocurrency* baru tiba-tiba meninggalkan proyek dan melarikan diri dengan membawa semua dana investor. Modusnya biasanya dimulai dengan menciptakan sebuah token baru (sering disebut *shitcoin* karena tidak memiliki nilai guna) dengan pemasaran yang masif di media sosial untuk menciptakan *hype*. Mereka kemudian menyediakan likuiditas di sebuah *Decentralized Exchange* (DEX), memungkinkan publik untuk membeli token mereka dengan menukarkan koin yang lebih berharga seperti Ethereum.

Setelah dana investor terkumpul dalam jumlah besar di dalam *liquidity pool*, para pengembang akan mengeksekusi penipuan mereka. Mereka menggunakan akses administratif yang mereka miliki untuk menarik semua aset berharga (misalnya, Ethereum) dari *pool* tersebut, meninggalkan investor dengan token tidak berharga yang nilainya langsung anjlok ke nol. Karena tim pengembangnya sering kali anonim dan *smart contract*-nya tidak diaudit, tidak ada pihak yang dapat dimintai pertanggungjawaban. Kerugian akibat *rug pull* telah mencapai miliaran dolar dan menjadi salah satu risiko terbesar bagi investor ritel di ekosistem DeFi (Chainalysis, 2022).

Selain *rug pull*, ada pula penawaran koin palsu yang meniru proyek-proyek besar yang sudah ada. Penipu akan membuat token dengan nama dan logo yang sangat mirip dengan koin populer, lalu menawarkannya dengan harga diskon melalui situs web palsu atau pesan langsung. Korban yang tidak teliti akan mentransfer dana mereka dengan harapan mendapatkan koin asli, namun yang mereka terima adalah token palsu yang tidak memiliki nilai sama sekali. Modus ini mengeksploitasi kurangnya pemahaman teknis korban mengenai bagaimana memverifikasi alamat kontrak token yang sah di *blockchain explorer*.

3. Phishing: Pencurian Kunci Pribadi (*Private Key*) dan Kredensial

Phishing adalah teknik rekayasa sosial yang bertujuan untuk mencuri informasi sensitif korban, seperti kata sandi, kredensial login, atau yang paling krusial dalam dunia kripto: *private key* atau *seed phrase*. *Private key* adalah kunci rahasia yang memberikan kontrol penuh atas aset di dalam sebuah dompet digital. Siapa pun yang memilikinya dapat menguras seluruh isinya. Penipu menggunakan berbagai cara untuk mendapatkan kunci ini. Salah satu metode yang umum adalah membuat situs web palsu yang meniru tampilan bursa kripto atau dompet web populer (misalnya, MetaMask atau Phantom).

Pelaku kemudian menyebarkan tautan ke situs palsu ini melalui email, media sosial, atau pesan pribadi, sering kali dengan dalih adanya "airdrop gratis", "pembaruan keamanan", atau "masalah pada akun" yang memerlukan tindakan segera. Korban yang panik atau tergiur akan mengklik tautan tersebut dan masuk ke situs palsu. Ketika mereka memasukkan kredensial login atau, yang lebih parah, *seed phrase* mereka, data tersebut

akan langsung terkirim ke penipu. Dalam hitungan detik, penipu akan menggunakan informasi tersebut untuk mengakses dompet korban dan mentransfer semua asetnya ke dompet mereka.

Metode *phishing* lainnya adalah melalui *malware*. Pelaku dapat menyisipkan perangkat lunak jahat ke dalam aplikasi atau file yang diunduh korban. *Malware* ini dapat berfungsi sebagai *keylogger* yang merekam setiap ketikan (termasuk kata sandi dan *private key*) atau secara aktif memindai file di komputer untuk mencari data dompet digital. Karena sifat transaksi kripto yang tidak dapat dibatalkan, aset yang telah dicuri melalui *phishing* hampir tidak mungkin untuk dikembalikan, menjadikannya salah satu ancaman paling langsung dan merusak bagi pengguna individu.

4. Studi Kasus Penipuan Investasi Kripto di Indonesia

Indonesia tidak luput dari maraknya penipuan berkedok investasi kripto. Salah satu kasus yang menonjol adalah platform robot trading Fahrenheit yang memakan korban ribuan anggota dengan total kerugian ditaksir mencapai triliunan rupiah pada tahun 2022. Platform ini menggunakan skema Ponzi yang canggih, menjanjikan keuntungan konsisten melalui robot trading aset kripto. Para anggota diiming-imingi keuntungan pasif yang besar dan didorong untuk merekrut anggota baru dengan bonus afiliasi yang menggiurkan, yang merupakan ciri khas skema piramida.

Para pelaku membangun citra kemewahan dan kesuksesan untuk menarik korban, memamerkan kekayaan yang seolah-olah berasal dari keuntungan trading. Namun, pada kenyataannya, dana dari anggota baru digunakan untuk membayar keuntungan anggota lama. Ketika platform tersebut tidak lagi mampu menarik anggota baru dalam jumlah yang cukup, sistemnya runtuh. Para petinggi perusahaan tiba-tiba menghentikan semua proses penarikan dana (*withdrawal*) dengan berbagai alasan teknis, sebelum akhirnya menghilang dan membawa kabur sisa dana investor.

Kasus ini menjadi pelajaran penting mengenai bahaya investasi bodong di sektor aset digital. Bareskrim Polri berhasil menangkap beberapa tersangka utama, menunjukkan bahwa meskipun pelaku menggunakan kripto, penegakan hukum masih dapat berjalan. Namun, kasus ini juga menyoroti kerentanan masyarakat Indonesia terhadap janji keuntungan

instan dan kurangnya literasi dalam membedakan antara investasi yang sah dan skema penipuan. Kerugian finansial yang masif dan trauma psikologis yang dialami para korban menegaskan urgensi edukasi publik dan pengawasan yang lebih ketat terhadap platform-platform serupa.

B. Pencucian Uang (*Money Laundering*)

Pencucian uang adalah proses menyamarkan asal-usul dana yang diperoleh secara ilegal agar tampak seolah-olah berasal dari sumber yang sah. *Cryptocurrency* telah menjadi alat yang sangat menarik bagi para pelaku pencucian uang karena karakteristiknya yang memungkinkan transfer nilai secara cepat, global, dan dengan tingkat anonimitas yang tinggi. Sub-bab ini akan menguraikan mekanisme pencucian uang menggunakan aset kripto, peran teknologi pengabur jejak seperti *mixer*, dan fungsi bursa tidak teregulasi sebagai pintu keluar-masuk dana ilegal.

1. Mekanisme Pencucian Uang melalui Cryptocurrency

Proses pencucian uang secara umum terdiri dari tiga tahap: penempatan (*placement*), pelapisan (*layering*), dan integrasi (*integration*). *Cryptocurrency* dapat digunakan dalam ketiga tahap tersebut. Pada tahap *placement*, pelaku kejahatan membeli aset kripto seperti Bitcoin atau Ethereum menggunakan uang tunai hasil kejahatan. Pembelian ini bisa dilakukan melalui transaksi *peer-to-peer* (P2P) atau melalui ATM kripto untuk menghindari sistem perbankan formal. Setelah dana ilegal berhasil diubah menjadi aset kripto, pelaku memasuki tahap *layering*.

Tahap *layering* adalah inti dari proses pencucian uang, di mana pelaku melakukan serangkaian transaksi yang rumit untuk mengaburkan jejak dan memutus hubungan antara aset kripto dengan sumber ilegalnya. Pelaku akan memindahkan dana melalui ratusan atau ribuan alamat dompet yang berbeda, menukarnya dengan berbagai jenis altcoin (proses yang disebut *chain hopping*), dan memanfaatkan layanan-layanan khusus untuk mempersulit pelacakan. Tujuannya adalah untuk membuat analisis *blockchain* menjadi sangat sulit, sehingga dana tersebut tampak bersih.

Pada tahap akhir, *integration*, dana yang telah "dicuci" dimasukkan kembali ke dalam sistem keuangan yang sah. Pelaku akan menjual aset

kripto mereka di bursa dan menarik hasilnya dalam bentuk uang fiat ke rekening bank. Mereka juga bisa menggunakan dana kripto tersebut untuk membeli barang-barang mewah, properti, atau aset lainnya secara langsung dari pedagang yang menerima pembayaran kripto. Dengan demikian, dana hasil kejahatan telah berhasil diintegrasikan ke dalam ekonomi legal tanpa terdeteksi sumber aslinya.

2. Penggunaan Mixer dan Tumbler untuk Mengaburkan Jejak Transaksi

Untuk meningkatkan efektivitas tahap *layering*, para pelaku pencucian uang sering kali menggunakan layanan yang disebut *mixer* atau *tumbler*. *Mixer* adalah layanan pihak ketiga (baik terpusat maupun terdesentralisasi) yang bekerja dengan cara mencampurkan dana kripto dari berbagai pengguna yang berbeda dalam satu *pool* besar. Setelah proses pencampuran, layanan ini akan mengirimkan kembali dana ke alamat baru yang disediakan oleh pengguna, dengan jumlah yang sama dengan yang mereka setorkan (dikurangi biaya layanan), tetapi menggunakan koin yang berasal dari pengguna lain.

Proses ini secara efektif memutus jejak transaksi di *blockchain*. Meskipun analisis *blockchain* dapat melihat bahwa sejumlah dana masuk ke alamat *mixer* dan sejumlah dana keluar dari *mixer*, sangat sulit untuk membuktikan secara definitif bahwa dana yang keluar adalah milik pengguna yang sama dengan dana yang masuk. Layanan seperti Tornado Cash (sebelum dikenai sanksi oleh otoritas AS) menjadi sangat populer karena menggunakan *smart contract* untuk mengotomatisasi proses ini secara terdesentralisasi, membuatnya lebih sulit untuk ditutup.

Penggunaan *mixer* merupakan tantangan besar bagi para analis forensik *blockchain* dan penegak hukum. Meskipun bursa-bursa besar yang teregulasi sering kali menandai dan menolak dana yang berasal dari alamat *mixer* yang diketahui, para pelaku kejahatan terus mencari cara baru untuk mengaburkan jejak mereka. Keberadaan layanan ini menunjukkan adanya "perlombaan senjata" teknologi yang konstan antara pihak yang mencoba menyembunyikan transaksi dan pihak yang mencoba mengungkapnya.

3. Peran Bursa Kripto Tanpa Regulasi (Unregulated Exchanges)

Bursa kripto (*crypto exchange*) adalah platform tempat pengguna dapat membeli, menjual, dan menukar aset kripto. Bursa yang teregulasi di yurisdiksi yang kuat (seperti Amerika Serikat atau Uni Eropa) diwajibkan untuk mematuhi aturan *Anti-Money Laundering* (AML) dan *Know Your Customer* (KYC). Ini berarti mereka harus mengumpulkan dan memverifikasi data identitas pengguna mereka, memantau transaksi yang mencurigakan, dan melaporkannya kepada pihak berwenang. Kepatuhan ini membuat bursa teregulasi menjadi tempat yang berisiko bagi para pelaku pencucian uang.

Oleh karena itu, bursa tanpa regulasi atau yang beroperasi di yurisdiksi dengan pengawasan AML/KYC yang lemah menjadi komponen vital dalam ekosistem pencucian uang kripto. Bursa-bursa ini sering kali tidak memerlukan verifikasi identitas sama sekali atau hanya memerlukan alamat email, memungkinkan siapa saja untuk membuka akun secara anonim. Para pelaku kejahatan memanfaatkan bursa ini sebagai titik masuk (*on-ramp*) untuk mengubah uang fiat menjadi kripto atau, yang lebih penting, sebagai titik keluar (*off-ramp*) untuk mengubah kripto yang sudah dicuci kembali menjadi uang fiat.

Menurut laporan dari perusahaan analisis *blockchain*, sebagian besar dana ilegal yang dicuci melalui *cryptocurrency* pada akhirnya mengalir ke segelintir bursa tidak teregulasi ini (Chainalysis, 2022). Bursa-bursa ini secara efektif berfungsi sebagai "lubang hitam" dalam sistem keuangan digital, menyerap dana dari sumber-sumber terlarang dan mempersulit upaya global untuk memerangi kejahatan keuangan. Tekanan internasional melalui lembaga seperti FATF (Financial Action Task Force) terus mendorong negara-negara untuk menerapkan regulasi yang ketat pada semua penyedia layanan aset virtual (VASP) untuk menutup celah ini.

4. Studi Kasus Penggunaan Kripto untuk Pencucian Uang

Salah satu studi kasus global yang paling terkenal terkait pencucian uang menggunakan *cryptocurrency* adalah peretasan bursa Bitfinex pada tahun 2016, di mana sekitar 120.000 Bitcoin dicuri. Selama bertahun-tahun, para peretas berusaha mencuci dana hasil curian tersebut. Analisis

blockchain menunjukkan bagaimana mereka menggunakan teknik *layering* yang sangat kompleks, memecah dana ke dalam ribuan transaksi kecil dan memindahkannya melalui berbagai alamat dan platform, termasuk pasar gelap AlphaBay.

Pada tahun 2022, Departemen Kehakiman AS berhasil menangkap sepasang suami istri, Ilya Lichtenstein dan Heather Morgan, dan menyita sekitar 94.000 Bitcoin (bernilai miliaran dolar pada saat itu) yang terkait dengan peretasan tersebut. Penangkapan ini menjadi kemenangan besar bagi penegak hukum dan membuktikan bahwa meskipun sangat sulit, transaksi kripto tidak sepenuhnya anonim dan dapat dilacak dengan teknik analisis forensik yang canggih. Kasus ini menunjukkan bahwa buku besar *blockchain* yang bersifat permanen dan publik dapat menjadi pedang bermata dua bagi para penjahat.

Di Indonesia, kasus-kasus pencucian uang menggunakan kripto juga mulai terungkap, meskipun sering kali terkait dengan kejahatan asal (*predicate crime*) seperti penipuan investasi atau narkotika. Para pelaku kejahatan di Indonesia diketahui membeli aset kripto untuk menyembunyikan hasil kejahatan mereka, lalu mengirimkannya ke bursa di luar negeri untuk dicairkan. PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan) telah berulang kali menyoroti peningkatan risiko pencucian uang melalui aset kripto dan bekerja sama dengan penyedia jasa keuangan kripto yang terdaftar untuk memantau dan melaporkan transaksi yang mencurigakan.

C. Pendanaan Terorisme (*Terrorism Financing*)

Pendanaan terorisme adalah penyediaan atau pengumpulan dana, baik secara langsung maupun tidak langsung, dengan maksud agar dana tersebut digunakan atau dengan pengetahuan bahwa dana tersebut akan digunakan untuk melakukan aksi terorisme. Kemampuan *cryptocurrency* untuk memfasilitasi transfer dana lintas batas dengan cepat dan dengan tingkat anonimitas tertentu telah menarik perhatian kelompok-kelompok teroris. Sub-bab ini akan menganalisis alasan di balik pergeseran ini, metode yang digunakan, serta tantangan besar yang dihadapi oleh aparat penegak hukum dalam melacak dan mencegahnya.

1. Alasan Teroris Beralih ke Cryptocurrency

Kelompok teroris secara tradisional mengandalkan metode pendanaan konvensional seperti sistem hawala, penyelundupan uang tunai, atau penyalahgunaan lembaga amal. Namun, metode-metode ini semakin berada di bawah pengawasan ketat dari intelijen keuangan global pasca serangan 11 September 2001. Sebagai respons, beberapa kelompok mulai bereksperimen dengan *cryptocurrency* karena beberapa keunggulan yang ditawarkannya. Pertama, sifatnya yang terdesentralisasi berarti tidak ada bank atau lembaga keuangan pusat yang dapat memblokir transaksi mereka.

Kedua, transaksi kripto bersifat lintas batas (*borderless*), memungkinkan mereka untuk mengirim dan menerima dana dari simpatisan di seluruh dunia tanpa melalui jalur perbankan formal yang memerlukan pemeriksaan identitas dan pelaporan. Ketiga, tingkat pseudonimitas yang ditawarkan oleh *cryptocurrency* seperti Bitcoin, dan anonimitas yang lebih kuat dari *privacy coins*, memberikan lapisan perlindungan bagi identitas donatur dan penerima. Meskipun jumlah dana yang terkumpul melalui kripto masih relatif kecil dibandingkan metode tradisional, tren penggunaannya terus meningkat dan menjadi perhatian serius bagi badan-badan anti-terorisme.

Kelompok-kelompok seperti ISIS dan Al-Qaeda diketahui telah secara aktif mempromosikan penggunaan *cryptocurrency* di saluran propaganda online mereka. Mereka mempublikasikan alamat donasi dalam bentuk Bitcoin dan mata uang kripto lainnya, serta memberikan tutorial kepada para pendukungnya tentang cara membeli dan mengirimkan kripto secara anonim. Kemudahan akses dan jangkauan global ini memungkinkan mereka untuk melakukan penggalangan dana mikro dari sejumlah besar simpatisan di berbagai negara, sebuah model yang sulit dideteksi dan diinterupsi oleh sistem keuangan tradisional.

2. Metode Penggalangan dan Transfer Dana Lintas Batas

Metode yang digunakan oleh kelompok teroris untuk menggalang dana melalui *cryptocurrency* terus berkembang. Awalnya, mereka hanya mempublikasikan alamat donasi statis di situs web atau saluran media sosial mereka. Namun, metode ini relatif mudah dilacak oleh analis *blockchain*,

yang dapat memantau semua dana yang masuk ke alamat tersebut. Untuk mengatasi ini, mereka mulai menggunakan teknik yang lebih canggih, seperti membuat alamat donasi baru untuk setiap donatur atau transaksi, sehingga mempersulit pemetaan jaringan pendanaan mereka.

Setelah dana terkumpul di beberapa dompet digital, langkah selanjutnya adalah mentransfernya ke sel-sel operatif di lapangan. Di sinilah kemampuan transaksi lintas batas kripto menjadi sangat berguna. Dana dapat dikirim dari Eropa atau Asia Tenggara ke zona konflik di Timur Tengah dalam hitungan menit, hanya dengan biaya transaksi jaringan. Untuk mencairkan dana tersebut menjadi uang tunai (*cash-out*), para operatif di lapangan dapat menggunakan berbagai cara, seperti platform P2P lokal, bertemu langsung dengan pialang kripto informal, atau menggunakan bursa di yurisdiksi dengan pengawasan yang lemah.

Selain donasi langsung, kelompok teroris juga dapat memanfaatkan *cryptocurrency* untuk menghasilkan pendapatan. Mereka dapat terlibat dalam aktivitas kriminal siber seperti peretasan atau penyebaran *ransomware* dan meminta tebusan dalam bentuk kripto. Mereka juga bisa melakukan penipuan investasi atau skema Ponzi yang menargetkan komunitas simpatisan mereka, dengan dalih bahwa "investasi" tersebut adalah bentuk jihad finansial. Diversifikasi sumber pendanaan ini membuat mereka lebih tangguh dan sulit untuk dilumpuhkan secara finansial.

3. Tantangan Pelacakan oleh Aparat Penegak Hukum

Meskipun *blockchain* bersifat transparan, melacak pendanaan terorisme menggunakan *cryptocurrency* menghadirkan tantangan unik bagi penegak hukum. Tantangan pertama adalah atribusi, yaitu menghubungkan sebuah alamat dompet digital dengan individu atau kelompok teroris di dunia nyata. Para pelaku menggunakan berbagai teknik untuk menyembunyikan identitas mereka, seperti menggunakan VPN, jaringan Tor, dan mendaftar di bursa dengan identitas palsu atau curian.

Tantangan kedua adalah kecepatan dan sifat global dari transaksi. Dana dapat bergerak melintasi beberapa negara dan yurisdiksi dalam hitungan jam, membuat koordinasi internasional antar lembaga penegak hukum menjadi sangat krusial namun juga sulit. Ketika dana sampai di yurisdiksi

yang tidak kooperatif atau tidak memiliki kapasitas untuk melakukan investigasi *blockchain*, jejaknya bisa menjadi dingin. Penggunaan *mixer*, *tumbler*, dan *privacy coins* semakin memperumit upaya pelacakan, menciptakan "lubang hitam" dalam analisis forensik.

Tantangan ketiga adalah pada titik *off-ramp* atau pencairan. Para teroris sering kali mencairkan dana dalam jumlah kecil melalui berbagai platform P2P atau pialang informal untuk menghindari deteksi. Mengidentifikasi dan menindak para pialang informal ini, yang sering beroperasi di tingkat lokal dan di luar sistem formal, merupakan pekerjaan yang sangat sulit. Untuk mengatasi tantangan ini, lembaga penegak hukum dan intelijen keuangan harus berinvestasi besar dalam teknologi analisis *blockchain*, membangun kapasitas sumber daya manusia, dan memperkuat kerja sama internasional untuk berbagi informasi secara *real-time*.

4. Analisis Kasus Global Pendanaan Terorisme via Kripto

Beberapa kasus global telah menyoroti penggunaan nyata *cryptocurrency* dalam pendanaan terorisme. Pada tahun 2020, Departemen Kehakiman AS mengumumkan pembongkaran tiga kampanye pendanaan terorisme siber yang melibatkan Brigade Al-Qassam (sayap militer Hamas), Al-Qaeda, dan ISIS. Kampanye-kampanye ini menggunakan media sosial dan situs web untuk meminta donasi dalam bentuk Bitcoin. Penegak hukum AS berhasil melacak dan menyita jutaan dolar dari lebih dari 300 alamat *cryptocurrency* yang terkait dengan kelompok-kelompok tersebut.

Dalam kasus ISIS, kelompok ini melancarkan kampanye penipuan yang canggih, membuat situs web palsu yang seolah-olah menjual alat pelindung diri (APD) selama puncak pandemi COVID-19. Pembayaran diminta dalam bentuk kripto, namun barang tidak pernah dikirim. Dana hasil penipuan ini kemudian dialihkan untuk mendanai aktivitas kelompok. Penyelidikan ini menunjukkan kemampuan penegak hukum untuk mengikuti jejak uang digital, menganalisis *blockchain*, dan bekerja sama dengan sektor swasta (bursa kripto) untuk mengidentifikasi dan menyita dana ilegal.

Kasus lain yang signifikan terjadi di Indonesia, di mana Densus 88 Antiteror Polri mengungkap bahwa seorang terduga teroris yang ditangkap pada tahun 2019 menggunakan Bitcoin untuk mengirimkan dana ke Suriah. Pelaku membeli Bitcoin melalui sebuah bursa kripto di Indonesia, lalu

mentransfernya ke alamat dompet yang dikendalikan oleh afiliasi ISIS di Suriah. Kasus ini menjadi bukti konkret pertama bahwa sel-sel teroris di Indonesia telah mulai mengadopsi *cryptocurrency* untuk pendanaan. Hal ini mendorong regulator dan penegak hukum di Indonesia untuk meningkatkan pengawasan terhadap transaksi aset kripto.

D. Peretasan (*Hacking*) dan Pencurian Aset Digital

Industri *cryptocurrency*, dengan nilai total yang mencapai triliunan dolar, telah menjadi target yang sangat menggiurkan bagi para peretas. Berbeda dengan sistem perbankan tradisional yang memiliki banyak lapisan keamanan dan asuransi, ekosistem digital ini sering kali memiliki titik-titik lemah yang dapat dieksploitasi. Sub-bab ini akan mengkategorikan berbagai jenis serangan siber, mulai dari peretasan skala besar terhadap bursa, pencurian dari dompet individu, hingga eksploitasi *smart contract* yang canggih di dunia DeFi.

1. Serangan terhadap Bursa Kripto (*Exchange Hacks*)

Bursa kripto adalah target utama bagi para peretas karena mereka menyimpan aset digital dalam jumlah sangat besar milik jutaan penggunanya. Peretasan bursa biasanya menargetkan *hot wallet*, yaitu dompet digital yang terhubung ke internet untuk memfasilitasi penarikan dana oleh pengguna secara cepat. Meskipun praktis, konektivitas online ini membuatnya rentan terhadap serangan. Peretas menggunakan berbagai vektor serangan, seperti *phishing* terhadap karyawan bursa untuk mencuri kredensial akses, mengeksploitasi kerentanan dalam perangkat lunak server, atau serangan rekayasa sosial.

Sejarah industri kripto diwarnai oleh serangkaian peretasan bursa yang spektakuler. Salah satu yang paling awal dan paling terkenal adalah peretasan Mt. Gox pada tahun 2014, yang kehilangan ratusan ribu Bitcoin dan menyebabkan keruntuhan bursa tersebut. Kasus yang lebih baru termasuk peretasan Binance pada 2019 dan KuCoin pada 2020. Meskipun bursa-bursa besar telah meningkatkan keamanan mereka secara signifikan, misalnya dengan menyimpan sebagian besar dana di *cold wallet* (dompet offline) dan menyediakan dana asuransi (SAFU - Secure Asset Fund for Users), risiko peretasan tidak pernah bisa dihilangkan sepenuhnya.

Kelompok peretas yang disponsori oleh negara, seperti Lazarus Group dari Korea Utara, telah diidentifikasi sebagai pelaku di balik banyak peretasan bursa. Mereka menggunakan hasil curian tersebut untuk mendanai program senjata negara mereka, menghindari sanksi internasional. Serangan-serangan ini tidak hanya menyebabkan kerugian finansial yang masif bagi pengguna, tetapi juga merusak kepercayaan publik terhadap keamanan ekosistem *cryptocurrency* secara keseluruhan dan sering kali memicu tindakan keras dari regulator.

2. Peretasan Dompet Digital (*Wallet Hacks*) Individu

Selain menargetkan bursa, peretas juga secara aktif menargetkan pengguna individu. Aset yang disimpan dalam dompet pribadi (*non-custodial wallet*) dikendalikan sepenuhnya oleh pengguna melalui *private key* atau *seed phrase*. Meskipun ini memberikan kedaulatan finansial, ia juga memindahkan semua tanggung jawab keamanan ke pundak pengguna. Jika peretas berhasil mendapatkan *private key* tersebut, mereka dapat menguras seluruh aset tanpa bisa dihentikan. Metode yang paling umum digunakan untuk mencuri kunci pribadi adalah *phishing* dan penyebaran *malware*.

Malware pencuri kripto dirancang khusus untuk memindai komputer atau perangkat seluler korban untuk mencari file yang berisi informasi dompet atau untuk memantau *clipboard*. Ketika pengguna menyalin (*copy*) alamat dompet untuk melakukan transaksi, *malware* dapat secara diam-diam menggantinya dengan alamat dompet milik peretas. Korban yang tidak memeriksa ulang alamat tujuan sebelum mengirim akan tanpa sadar mentransfer dana mereka ke penipu. Jenis *malware* lain, yang dikenal sebagai *infostealer*, dapat mencuri semua kata sandi yang tersimpan di browser, termasuk akses ke akun bursa kripto.

Untuk melindungi diri, pengguna disarankan untuk menggunakan *hardware wallet*. Ini adalah perangkat fisik kecil yang menyimpan *private key* secara offline, terisolasi dari komputer atau ponsel yang rentan terhadap *malware*. Transaksi harus ditandatangani secara manual dengan menekan tombol pada perangkat itu sendiri, memberikan lapisan keamanan tambahan yang signifikan. Namun, bahkan pengguna *hardware wallet* pun tidak kebal jika mereka tertipu untuk memasukkan *seed phrase* mereka di situs *phishing*.

3. Eksploitasi Kerentanan dalam *Smart Contract* (DeFi Hacks)

Munculnya Keuangan Terdesentralisasi (DeFi) telah membuka vektor serangan baru yang sangat canggih: eksploitasi kerentanan dalam *smart contract*. Protokol DeFi adalah aplikasi keuangan yang berjalan di atas *blockchain* dan diatur oleh kode komputer (*smart contract*). Jika ada cacat atau celah logika dalam kode tersebut, peretas dapat mengeksploitasinya untuk memanipulasi protokol dan menguras dana yang terkunci di dalamnya. Jenis serangan ini sering kali sangat teknis dan sulit dipahami oleh orang awam.

Beberapa jenis eksploitasi yang umum terjadi antara lain *re-entrancy attack*, di mana peretas berulang kali menarik dana dari sebuah protokol sebelum saldo mereka diperbarui. Ada pula *flash loan attack*, di mana peretas meminjam sejumlah besar aset kripto tanpa agunan (hanya untuk durasi satu blok transaksi), menggunakannya untuk memanipulasi harga di sebuah protokol DeFi, mendapatkan keuntungan besar, dan kemudian mengembalikan pinjaman kilat tersebut, semuanya dalam satu transaksi atomik. Serangan-serangan ini mengeksploitasi cara kerja protokol DeFi yang saling terhubung (*composability*).

Kerugian akibat peretasan DeFi telah melampaui angka miliaran dolar setiap tahunnya, menjadikannya kategori peretasan kripto yang paling merusak saat ini (Chainalysis, 2022). Kasus-kasus terkenal seperti peretasan The DAO pada tahun 2016, Poly Network pada tahun 2021, dan Wormhole pada tahun 2022 menunjukkan betapa berbahayanya kerentanan dalam kode. Hal ini menggarisbawahi pentingnya audit keamanan *smart contract* oleh firma-firma terkemuka sebelum sebuah protokol diluncurkan. Namun, bahkan audit pun tidak dapat menjamin keamanan 100%, dan risiko kode akan selalu ada dalam ekosistem DeFi.

4. Kerugian Finansial Akibat Peretasan di Industri Kripto

Dampak kumulatif dari berbagai jenis peretasan ini sangat signifikan. Menurut laporan dari berbagai firma analisis *blockchain* dan keamanan siber, total kerugian akibat peretasan dan penipuan di industri kripto sejak awal kemunculannya telah mencapai puluhan miliar dolar. Angka ini terus meningkat setiap tahun seiring dengan pertumbuhan nilai pasar

dan kompleksitas ekosistem. Kerugian ini tidak hanya berupa angka di neraca, tetapi juga mewakili hilangnya tabungan dan investasi dari jutaan individu di seluruh dunia.

Kerugian finansial ini memiliki efek riak. Peretasan besar dapat menyebabkan runtuhnya sebuah bursa atau protokol DeFi, yang pada gilirannya dapat memicu kepanikan pasar dan penurunan harga aset secara luas. Hal ini juga mengikis kepercayaan investor institusional dan ritel untuk masuk ke dalam ekosistem, menghambat adopsi massal. Selain itu, frekuensi peretasan yang tinggi menjadi alasan utama bagi regulator di seluruh dunia untuk memberlakukan aturan yang lebih ketat pada industri ini, yang terkadang dapat menghambat inovasi.

Berbeda dengan sistem perbankan tradisional di mana simpanan nasabah sering kali diasuransikan oleh pemerintah (seperti LPS di Indonesia atau FDIC di AS), di dunia kripto, perlindungan semacam itu umumnya tidak ada. Ketika aset dicuri dari dompet pribadi atau dari bursa yang tidak memiliki dana asuransi, dana tersebut hilang selamanya. Sifat transaksi yang *irreversible* membuat pemulihan hampir tidak mungkin dilakukan. Realitas pahit ini menekankan prinsip utama di dunia kripto: *Not your keys, not your coins*, dan pentingnya setiap individu untuk bertanggung jawab penuh atas keamanan aset digital mereka.

E. Kejahatan di Pasar Gelap (*Dark Web*)

Dark web adalah bagian dari internet yang tidak terindeks oleh mesin pencari konvensional dan hanya dapat diakses melalui perangkat lunak khusus seperti Tor (The Onion Router) untuk menjaga anonimitas pengguna. Sejak kemunculannya, *dark web* telah menjadi pusat bagi berbagai aktivitas ilegal. *Cryptocurrency*, khususnya Bitcoin, memainkan peran instrumental dalam memfasilitasi transaksi di pasar gelap ini. Sub-bab ini akan membahas peran sentral kripto di *dark web*, jenis barang dan jasa ilegal yang diperdagangkan, serta keterkaitan simbiosis antara kedua ekosistem ini.

1. Cryptocurrency sebagai Alat Transaksi Utama di Dark Web

Sebelum adanya Bitcoin, transaksi di pasar gelap online sangat sulit dan berisiko, sering kali bergantung pada metode pembayaran yang dapat dilacak seperti transfer bank atau kartu kredit. Kemunculan Bitcoin pada tahun 2009 menjadi sebuah revolusi bagi para operator pasar gelap. Bitcoin menawarkan solusi pembayaran yang memenuhi tiga kriteria penting bagi mereka: (1) digital dan dapat ditransfer secara instan melintasi batas negara; (2) terdesentralisasi, sehingga tidak dapat dibekukan atau disensor oleh pemerintah atau bank; dan (3) bersifat pseudonim, memberikan lapisan kerahasiaan bagi pembeli dan penjual.

Pasar gelap pertama yang mengadopsi Bitcoin secara massal adalah Silk Road, yang diluncurkan pada tahun 2011. Platform ini berfungsi seperti "Amazon untuk barang-barang ilegal", di mana penjual dapat mendaftar, memajang produk mereka, dan menerima pembayaran dalam bentuk Bitcoin. Silk Road menggunakan sistem reputasi dan layanan *escrow* (dana ditahan oleh platform hingga pembeli mengonfirmasi penerimaan barang) untuk membangun kepercayaan antara para pihak yang anonim. Keberhasilan Silk Road membuktikan kelayakan model bisnis ini dan memicu lahirnya puluhan pasar gelap lainnya.

Meskipun Bitcoin tetap menjadi yang paling populer karena likuiditasnya, banyak pasar gelap kemudian mulai mengadopsi *privacy coins* seperti Monero. Monero menawarkan anonimitas yang jauh lebih kuat daripada Bitcoin dengan menyembunyikan alamat pengirim, penerima, dan jumlah transaksi secara default. Pergeseran ke Monero ini merupakan respons terhadap semakin canggihnya kemampuan lembaga penegak hukum dalam melakukan analisis dan pelacakan transaksi Bitcoin di *blockchain*.

2. Perdagangan Narkotika, Senjata, dan Data Curian

Kategori produk yang paling dominan diperdagangkan di pasar gelap *dark web* adalah narkotika. Penjual dari seluruh dunia dapat menawarkan berbagai jenis zat terlarang, mulai dari ganja, kokain, hingga opioid sintetis, yang kemudian dikirimkan kepada pembeli melalui layanan pos konvensional dengan kemasan yang dirancang untuk menghindari

deteksi. Model ini memungkinkan pengguna untuk membeli narkotika dari kenyamanan rumah mereka tanpa harus berinteraksi langsung dengan pengedar di jalanan, yang mereka anggap lebih berisiko. Pembayaran untuk semua transaksi ini hampir secara eksklusif dilakukan menggunakan *cryptocurrency*.

Selain narkotika, pasar gelap juga menjadi tempat jual beli data curian dalam skala besar. Data ini biasanya berasal dari peretasan besar terhadap perusahaan atau lembaga pemerintah, dan dapat mencakup informasi kartu kredit, kredensial login untuk akun perbankan online, data pribadi (nama, alamat, nomor identitas), dan rekam medis. Para pelaku kejahatan siber lainnya membeli data ini untuk melakukan penipuan identitas, pengambilalihan akun, atau serangan *phishing* yang lebih tertarget. Harga data bervariasi tergantung pada kelengkapan dan kebaruannya.

Kategori barang berbahaya lainnya yang ditemukan di *dark web* adalah senjata api dan bahan peledak, meskipun perdagangannya tidak sebesar narkotika karena risiko pengiriman fisik yang jauh lebih tinggi. Selain itu, terdapat pula pasar untuk dokumen palsu (paspor, SIM), uang palsu, dan perangkat lunak peretasan. Semua perdagangan ini didukung oleh ekosistem pembayaran berbasis kripto, yang memungkinkan para penjahat untuk memonetisasi aktivitas ilegal mereka dengan tingkat anonimitas yang relatif tinggi.

3. Layanan Ilegal: Ransomware-as-a-Service

Salah satu perkembangan paling mengkhawatirkan di ekosistem kejahatan siber adalah munculnya model bisnis *Ransomware-as-a-Service* (RaaS). RaaS adalah model afiliasi di mana para pengembang *ransomware* (operator) menyewakan *malware* mereka kepada pihak lain (afiliasi). Afiliasi inilah yang kemudian bertanggung jawab untuk menyebarkan *ransomware* dan menginfeksi jaringan korban, misalnya melalui email *phishing* atau eksploitasi kerentanan server. Jika korban membayar uang tebusan, hasilnya akan dibagi antara operator dan afiliasi, sering kali dengan porsi terbesar (misalnya, 70-80%) diberikan kepada afiliasi.

Model RaaS ini secara drastis menurunkan ambang batas teknis untuk menjadi seorang penjahat siber. Seseorang dengan keterampilan peretasan yang terbatas kini dapat "menyewa" *ransomware* yang sangat canggih dan melancarkan serangan terhadap perusahaan besar, rumah sakit, atau bahkan infrastruktur kritis. Seluruh ekosistem RaaS ini berjalan di atas *cryptocurrency*. Pembayaran uang tebusan hampir selalu diminta dalam bentuk Bitcoin atau Monero karena sifatnya yang sulit dilacak dan tidak dapat dibatalkan.

Portal RaaS yang beroperasi di *dark web* menyediakan dasbor bagi para afiliasi untuk melacak infeksi, berkomunikasi dengan korban, dan menerima bagian pembayaran tebusan mereka. Ini menciptakan ekonomi bawah tanah yang sangat profesional dan terorganisir. Keberhasilan model RaaS telah menyebabkan ledakan jumlah serangan *ransomware* di seluruh dunia, menyebabkan kerugian miliaran dolar dan gangguan layanan yang parah di berbagai sektor.

4. Keterkaitan antara Pasar Gelap dan Ekosistem Kripto

Terdapat hubungan simbiosis yang erat antara pasar gelap di *dark web* dan ekosistem *cryptocurrency* secara umum. Di satu sisi, pasar gelap adalah salah satu kasus penggunaan (*use case*) awal yang membuktikan kelayakan *cryptocurrency* sebagai sistem pembayaran yang tahan sensor dan pseudonim. Aktivitas di *dark web* menciptakan permintaan yang konsisten untuk aset kripto, yang pada gilirannya berkontribusi pada likuiditas dan kesadaran akan teknologi tersebut, terutama pada tahun-tahun awalnya.

Di sisi lain, dana yang berasal dari aktivitas ilegal di *dark web* pada akhirnya harus dicuci dan diintegrasikan kembali ke dalam ekonomi yang sah. Ini menciptakan aliran dana ilegal yang signifikan ke dalam ekosistem kripto yang lebih luas. Para operator pasar gelap dan penjual menggunakan layanan *mixer* dan bursa tidak teregulasi—layanan yang sama yang digunakan oleh pelaku pencucian uang lainnya—untuk mengaburkan asal-usul dana mereka sebelum mencairkannya menjadi uang fiat. Jejak dana dari pasar gelap yang terkenal seperti AlphaBay atau Hydra sering kali dapat ditemukan mengalir ke bursa-bursa besar, yang menjadi tantangan bagi tim kepatuhan (*compliance*) mereka.

Meskipun volume transaksi di *dark web* hanya mewakili sebagian kecil dari total volume transaksi *cryptocurrency* global, reputasinya telah memberikan stigma negatif yang signifikan pada seluruh industri. Regulator dan penegak hukum sering kali menyoroti hubungan ini sebagai justifikasi untuk pengawasan yang lebih ketat. Bagi industri kripto, memisahkan diri dari citra kejahatan dan pasar gelap merupakan tantangan berkelanjutan dalam upaya mereka untuk mencapai legitimasi dan adopsi oleh masyarakat umum.

Analisis Mendalam Konsep Kunci Bab 4: Tipologi Modus Operandi Kejahatan Kripto

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk mengubah pemahaman abstrak tentang "kejahatan kripto" menjadi sebuah katalog modus operandi yang terstruktur dan konkret. Tujuannya adalah untuk:

1. Mengedukasi: Memberikan pemahaman yang jelas kepada pembaca (terutama yang awam) tentang berbagai cara mereka bisa menjadi korban.
2. Mengkategorikan: Mengelompokkan kejahatan berdasarkan niat dan metode pelaku (misalnya, menipu untuk mendapatkan uang vs. menyembunyikan uang haram).
3. Menyediakan Dasar Analisis Hukum: Setiap kategori kejahatan ini akan menjadi "objek" yang akan dianalisis menggunakan "pisau" hukum pidana Islam (di Bab 5 dan 9) dan hukum positif (di Bab 6 dan 8).

Tanpa tipologi yang jelas, pembahasan tentang penanggulangan kejahatan akan menjadi kabur dan tidak terarah. Bab 4 menyediakan "daftar target" yang spesifik.

Elemen-Elemen Kunci dalam Tipologi:

1. Vektor Serangan: Bagaimana pelaku berinteraksi dengan korban atau sistem? (Melalui rekayasa sosial, eksploitasi teknis, atau penyalahgunaan platform?)
2. Aset yang Diincar: Apa yang menjadi target utama? (Uang fiat korban, aset kripto yang sudah dimiliki, atau penggunaan jaringan untuk tujuan lain?)
3. Teknologi yang Dieksploitasi: Fitur apa dari *cryptocurrency* yang dimanfaatkan? (Anonimitas, kecepatan transaksi lintas batas, atau sifatnya yang tidak teregulasi?)
4. Skala Dampak: Apakah dampaknya bersifat individual (pencurian dompet) atau sistemik (pencucian uang, pendanaan terorisme)?

Analisis Komparatif: Lima Tipologi Utama Kejahatan Kripto

Tabel berikut membedah lima kategori utama modus operandi yang dibahas dalam Bab 4, menyoroti perbedaan fundamental dalam metode dan tujuan mereka.

Fitur Kunci	Penipuan (*Scam*) & Investasi Bodong	Pencucian Uang (*Money Laundering*)	Pendanaan Terorisme	Peretasan (*Hacking*) & Pencurian	Pasar Gelap (*Dark Web*)
Tujuan Utama Pelaku	Mengeruk dana dari korban dengan janji-janji palsu.	Menyamarkan asal-usul dana hasil kejahatan agar terlihat sah.	Mengumpulkan & mentransfer dana untuk mendanai operasi teror.	Mencuri aset digital yang sudah ada dari dompet individu atau bursa.	Memfasilitasi transaksi ilegal untuk barang/ jasa terlarang.
Korban Utama	Publik/ Investor awam yang tergiur keuntungan tinggi.	Sistem Keuangan & Negara. Integritas sistem dirusak.	Masyarakat & Negara. Keamanan publik dan stabilitas nasional terancam.	Pemilik aset kripto & Platform Bursa Kripto.	Pengguna narkotika, korban r*ansomware*, dan masyarakat secara umum.
Vektor Serangan	Rekayasa Sosial: Pemasaran agresif, skema Ponzi, *phishing*, *rug pull*.	Penyalahgunaan Platform: Menggunakan bursa tanpa KYC, *mixer/tumbler*.	Penyalahgunaan Platform: Donasi anonim, transfer P2P lintas batas.	Eksploitasi Teknis: Meretas *smart contract*, mencuri *private key*, serangan pada bursa.	Penyalahgunaan Platform: Menggunakan kripto sebagai alat bayar di pasar anonim.
Fitur Kripto yang Dieksploitasi	Hype & Spekulasi. Mudah menciptakan token baru (*shitcoins*).	Pseudenonimitas & Kecepatan Transaksi Lintas Batas.	Pseudenonimitas & Sifat Tanpa Batas. Sulit dilacak tanpa analisis khusus.	Sifat Digital & Irreversibel. Aset yang dicuri sulit dikembalikan jika sudah dipindahkan.	Pseudenonimitas & Ketahanan Sensor. Transaksi tidak dapat diblokir oleh bank.
Contoh Modus Operandi	Robot trading (Fahrenheit), Penawaran Koin Palsu (ICO fiktif).	Memecah dana hasil korupsi ke banyak alamat, lalu menggunakan *mixer* sebelum dicairkan.	Menggalang dana melalui kanal media sosial, lalu mentransfernya ke afiliasi di negara lain.	Peretasan bursa Mt. Gox, peretasan Ronin Bridge (*Axie Infinity*).	Transaksi jual beli narkotika di Silk Road, pembayaran tebusan *ransomware*.

Kontribusi Konsep Tipologi dalam Bab 4:

Konsep ini berfungsi sebagai katalog kejahatan yang menjadi fondasi bagi seluruh bagian analisis hukum dalam buku ini.

1. Memberikan Struktur pada Masalah: Bab 4 mengubah "masalah kejahatan kripto" yang abstrak menjadi serangkaian masalah konkret yang dapat dianalisis satu per satu. Ini mencegah pembahasan menjadi terlalu umum.
2. Menjadi Objek Analisis Hukum: Setiap baris dalam tabel ini menjadi "studi kasus" teoretis. Bab 5 akan bertanya, "Bagaimana hukum pidana Islam mengkualifikasikan Penipuan (kolom 1)?" Bab 6 akan bertanya, "Pasal apa dalam UU TPPU yang bisa menjerat Pencucian Uang (kolom 2)?"
3. Menginformasikan Strategi Penanggulangan: Dengan memahami modus operandi yang berbeda, strategi penanggulangan (Bab 11 & 12) dapat dirancang secara lebih spesifik. Misalnya, strategi untuk melawan Penipuan adalah edukasi publik, sedangkan strategi untuk melawan Peretasan adalah peningkatan keamanan teknis.

Secara esensial, Bab 4 adalah jembatan antara bagian teori (Bab 1-3) dan bagian analisis hukum (Bab 5-10). Ia mengambil konsep *cryptocurrency* dan menunjukkan secara praktis bagaimana konsep tersebut dapat "dipelintir" untuk tujuan jahat. Dengan memetakan anatomi kejahatan ini, buku ini siap untuk membedahnya dengan pisau analisis hukum di bab-bab berikutnya.

BAB 5

Kualifikasi Kejahatan Cryptocurrency dalam Hukum Pidana Islam

Setelah memetakan lanskap kejahatan ekonomi digital pada Bab 4, kini kita tiba pada jantung analisis yuridis buku ini. Bab 5 bertujuan untuk "menerjemahkan" modus-modus operandi kejahatan modern tersebut ke dalam bahasa dan kerangka hukum pidana Islam. Pertanyaan fundamental yang dijawab bukanlah "apakah perbuatan ini salah?", karena secara intuitif jawabannya adalah iya, melainkan "bagaimana perbuatan ini diklasifikasikan dalam taksonomi *jarīmah* (tindak pidana Islam), dan apa implikasi hukumnya?". Dalam diskursus fikih kontemporer, sering terjadi keraguan apakah sistem hukum yang berakar pada tradisi mampu merespons kejahatan yang lahir dari teknologi mutakhir. *Research gap* yang diisi oleh bab ini adalah kurangnya analisis sistematis yang secara langsung melakukan *takhyīf fiqhī* (kualifikasi fikih) terhadap setiap modus kejahatan *cryptocurrency*. Pertanyaan penelitian utama bab ini adalah: Bagaimana tindak pidana penipuan, pencurian aset digital, pencucian uang, pendanaan terorisme, dan perdagangan ilegal yang menggunakan *cryptocurrency* dapat dikualifikasikan dan dianalisis berdasarkan kategori dan prinsip-prinsip *jarīmah hudūd*, *qiṣāṣ*, dan *ta'zīr* dalam hukum pidana Islam?

A. Penipuan sebagai Jarimah Ta'zir

Penipuan (*scam*) dalam berbagai bentuknya merupakan kejahatan yang paling lazim di ekosistem *cryptocurrency*. Sub-bab ini akan menganalisis bagaimana perbuatan ini dapat dikualifikasikan sebagai tindak pidana dalam hukum Islam. Dengan menggunakan metode analogi (*qiyās*), penipuan digital akan dibandingkan dengan konsep penipuan klasik dalam fikih. Pembahasan akan mencakup tantangan pembuktian unsur-unsur pidananya, ragam hukuman *ta'zīr* yang dapat diterapkan, serta landasan filosofisnya dalam kaidah fikih yang relevan.

1. Analogi (*Qiyas*) dengan Tindak Pidana Penipuan Klasik

Hukum pidana Islam tidak mendefinisikan penipuan sebagai salah satu kejahatan *hudūd*. Oleh karena itu, ia secara otomatis masuk ke dalam kategori *jarīmah ta'zīr*. Untuk memahami bagaimana penipuan kripto dikualifikasikan, kita dapat menganalogikannya (*qiyās*) dengan konsep-konsep penipuan yang telah dikenal dalam literatur fikih klasik. Konsep

yang paling relevan adalah *tadlīs* (menyembunyikan cacat atau memberikan informasi palsu), *ghishsh* (kecurangan), dan *khidā'* (tipu daya). Semua perbuatan ini secara tegas dilarang karena melanggar prinsip kejujuran dan kerelaan dalam bertransaksi (*'an tarāḍin minkum*). Skema Ponzi, *rug pull*, dan *phishing* pada esensinya adalah bentuk-bentuk *tadlīs* dan *khidā'* yang canggih.

Misalnya, dalam kasus *rug pull*, pengembang melakukan *tadlīs* dengan menciptakan citra proyek yang menjanjikan, padahal niat sesungguhnya adalah untuk melarikan diri dengan dana investor. Ini dianalogikan dengan seorang penjual di pasar klasik yang memoles barang dagangannya yang cacat agar terlihat bagus. Meskipun mediumnya berbeda (kode digital vs. barang fisik), *'illah* (alasan hukum) pelarangannya sama, yaitu adanya tipu daya yang menyebabkan kerugian finansial pada pihak lain. Dengan demikian, kejahatan-kejahatan ini dapat dikualifikasikan sebagai *jarīmah ta'zīr* atas dasar *qiyās* dan larangan umum memakan harta orang lain secara batil (*aklu amwāl al-nās bi al-bāṭil*).

Kualifikasi sebagai *jarīmah ta'zīr* memberikan fleksibilitas kepada negara (*ulil amri*) untuk merumuskan undang-undang spesifik yang melarang berbagai bentuk penipuan digital. Undang-undang seperti UU ITE di Indonesia, yang melarang penyebaran berita bohong yang merugikan konsumen dalam transaksi elektronik, dapat dipandang sebagai manifestasi modern dari penetapan *jarīmah ta'zīr*. Negara berwenang penuh untuk mendefinisikan perbuatan-perbuatan ini sebagai tindak pidana dan menetapkan sanksinya demi melindungi kemaslahatan umum, khususnya perlindungan terhadap harta (*ḥifẓ al-māl*).

2. Pembuktian Unsur Niat Jahat dan Kerugian Korban

Untuk menjatuhkan hukuman atas tindak pidana penipuan, ketiga rukun *jarīmah* harus terpenuhi dan dibuktikan. Rukun formal (*al-rukn al-syar'ī*) terpenuhi dengan adanya larangan dalam *nash* (baik larangan umum terhadap penipuan maupun undang-undang spesifik). Rukun materiil (*al-rukn al-maddī*) terpenuhi dengan adanya perbuatan (misalnya, membuat situs *phishing* atau meluncurkan skema Ponzi) dan akibat (hilangnya aset kripto milik korban). Namun, tantangan terbesar sering kali terletak pada pembuktian rukun moril (*al-rukn al-adabī*), yaitu niat jahat (*qaṣd jinā'ī* atau *niyyah*) dari pelaku.

Jaksa atau penuntut harus mampu membuktikan bahwa pelaku sejak awal memiliki niat untuk menipu, bukan sekadar proyek bisnis yang gagal secara wajar. Dalam konteks digital, pembuktian ini dapat dilakukan melalui jejak digital. Misalnya, pada kasus *rug pull*, niat jahat dapat diindikasikan dari anonimitas total tim pengembang, ketiadaan audit *smart contract*, atau adanya fungsi tersembunyi dalam kode yang memungkinkan pengembang untuk menarik semua dana. Dalam kasus *phishing*, pembuatan situs web palsu yang identik dengan aslinya sudah merupakan bukti kuat adanya niat untuk menipu.

Selain niat pelaku, kerugian yang dialami korban juga harus dibuktikan secara konkret. Dalam dunia kripto, ini dapat dilakukan dengan menunjukkan catatan transaksi di *blockchain* yang membuktikan bahwa sejumlah aset telah ditransfer dari dompet korban ke dompet yang dikendalikan oleh pelaku. Transparansi *blockchain* di sini justru dapat membantu proses pembuktian rukun materiil. Kesulitan muncul jika pelaku menggunakan *mixer* untuk mengaburkan jejak, namun setidaknya transfer awal dari korban ke pelaku dapat dibuktikan dengan jelas.

3. Bentuk Hukuman Ta'zir: Denda, Penjara, atau Publikasi Pelaku

Karena penipuan termasuk *jarīmah ta'zīr*, bentuk dan kadar hukumannya tidak ditetapkan secara kaku oleh *nash*, melainkan diserahkan pada kebijakan hakim (*qāḍī*) atau penguasa. Hakim memiliki diskresi luas untuk menjatuhkan hukuman yang dianggap paling efektif untuk mencapai tujuan pemidanaan, yaitu memberikan efek jera bagi pelaku (*deterrence*), menjadi pelajaran bagi masyarakat, dan memulihkan kerugian korban jika memungkinkan. Rentang hukuman *ta'zīr* sangat lebar, mulai dari yang paling ringan hingga yang paling berat.

Bentuk hukuman yang dapat diterapkan untuk penipu kripto antara lain adalah penjara (*al-ḥabs*), yang durasinya dapat disesuaikan dengan skala penipuan dan jumlah kerugian yang ditimbulkan. Hukuman denda (*al-gharāmah*) juga sangat relevan, di mana pelaku diwajibkan membayar sejumlah uang yang dapat digunakan untuk mengompensasi kerugian para korban. Dalam fikih Islam, perampasan aset hasil kejahatan untuk dikembalikan kepada pemiliknya adalah sebuah keharusan.

Selain itu, hakim dapat menerapkan bentuk hukuman lain yang bersifat mempermalukan pelaku di depan publik (*al-tashhīr*) sebagai efek jera tambahan. Dalam konteks modern, ini bisa berupa publikasi identitas dan kejahatan pelaku di media massa atau platform online. Tujuan dari variasi hukuman ini adalah untuk memastikan bahwa sanksi yang dijatuhkan bersifat proporsional, adil, dan mampu merespons tingkat bahaya sosial yang ditimbulkan oleh kejahatan tersebut, sejalan dengan semangat fleksibilitas dalam hukuman *ta'zīr*.

4. Kaidah Fikih: "Kemudaratan Harus Dihilangkan" (Al-Dharar Yuzal)

Landasan filosofis di balik kriminalisasi dan penghukuman terhadap penipuan dapat ditemukan dalam salah satu kaidah fikih fundamental (*al-qawā'id al-fiqhiyyah al-khamsah*), yaitu "*al-ḍarar yuzāl*" (kemudaratan atau kerugian harus dihilangkan). Kaidah ini menegaskan bahwa syariah bertujuan untuk menghilangkan segala bentuk bahaya dan kerugian, baik yang bersifat umum maupun khusus. Penipuan investasi kripto jelas menimbulkan *ḍarar* yang nyata, yaitu kerugian finansial bagi para korban dan rusaknya kepercayaan dalam ekosistem ekonomi digital.

Berdasarkan kaidah ini, negara tidak hanya berhak, tetapi juga berkewajiban untuk mengambil tindakan aktif untuk menghilangkan kemudaratan tersebut. Tindakan ini mencakup tiga level. Pertama, level preventif, yaitu dengan melakukan edukasi publik tentang bahaya investasi bodong dan memberlakukan regulasi yang ketat. Kedua, level penindakan, yaitu dengan menginvestigasi dan mengadili para pelaku penipuan serta menjatuhkan hukuman *ta'zīr* yang setimpal. Ketiga, level **restitutif**, yaitu dengan berupaya semaksimal mungkin untuk menyita aset hasil kejahatan dan mengembalikannya kepada para korban (*restitusi*).

Kaidah ini memberikan legitimasi syariah yang kuat bagi seluruh upaya negara dalam memberantas kejahatan penipuan. Ia menggeser paradigma dari sekadar menghukum pelaku menjadi sebuah pendekatan yang lebih holistik, yaitu menghilangkan sumber kemudaratan dan memulihkan kondisi yang adil. Dengan demikian, setiap kebijakan atau tindakan hukum yang bertujuan untuk memberantas penipuan kripto dapat dibenarkan sebagai implementasi dari kaidah "*al-ḍarar yuzāl*".

B. Pencurian (Sariqah) Aset Digital

Pencurian aset digital melalui peretasan (*hacking*) adalah kejahatan yang secara langsung merampas harta korban. Sub-bab ini akan menganalisis bagaimana perbuatan ini dikualifikasikan dalam hukum pidana Islam. Fokus utama adalah pada perdebatan apakah pencurian aset kripto dapat memenuhi syarat-syarat ketat dari *sariqah hudūd* (pencurian yang diancam dengan hukuman potong tangan). Pandangan mayoritas yang mengkategorikannya sebagai *jarīmah ta'zīr* akan dielaborasi, beserta pembahasan mengenai konsep *ḥirābah* untuk kasus peretasan skala besar.

1. Perdebatan Pemenuhan Syarat Sariqah Hudud (Nisab, Tempat Simpan)

Sariqah yang diancam dengan sanksi *hadd* (potong tangan) memiliki syarat-syarat yang sangat ketat yang harus terpenuhi tanpa keraguan sedikit pun. Di antara syarat utamanya adalah (1) barang yang dicuri harus mencapai *niṣāb* (batas minimum nilai tertentu, umumnya setara dengan seperempat dinar emas); (2) barang tersebut harus diambil dari *ḥirz* (tempat penyimpanan yang layak dan terkunci); dan (3) perbuatan tersebut harus dilakukan secara diam-diam dan sembunyi-sembunyi (Al-Mawardi, 1996). Perdebatan muncul ketika mencoba menerapkan syarat-syarat ini pada pencurian aset digital.

Syarat *niṣāb* mungkin mudah terpenuhi, karena nilai aset kripto yang dicuri sering kali jauh melampaui nilai seperempat dinar. Namun, perdebatan sengit terjadi pada konsep *ḥirz*. Apakah sebuah *digital wallet* (baik itu *hot wallet* di bursa atau *cold wallet* berupa perangkat keras) dapat dianggap sebagai *ḥirz* dalam pengertian klasik? Sebagian ulama berpendapat iya, karena ia dilindungi oleh lapisan keamanan seperti kata sandi dan enkripsi, yang berfungsi sebagai "gembok" digital. Namun, ulama lain berpendapat bahwa konsep *ḥirz* secara tradisional merujuk pada tempat penyimpanan fisik yang konkret, dan menganalogikannya dengan ruang digital yang abstrak akan menimbulkan *syubhat* (keraguan).

Keraguan lainnya adalah mengenai syarat "diambil secara diam-diam". Peretasan sering kali melibatkan manipulasi kode atau eksploitasi sistem, yang berbeda dengan tindakan fisik mengambil barang dari sebuah

tempat. Karena adanya berbagai *syubhat* dan kesulitan dalam menerapkan syarat-syarat klasik ini pada konteks digital, mayoritas ulama kontemporer berkesimpulan bahwa hukuman *hadd* untuk pencurian tidak dapat diterapkan pada kasus peretasan aset digital. Kaidah fikih menyatakan "*idra'ū al-ḥudūd bi al-shubuhāt*" (tolaklah pelaksanaan hukuman *hudūd* apabila terdapat keraguan).

2. Pandangan Mayoritas: Pencurian Aset Digital sebagai Jarimah Ta'zir

Karena tidak terpenuhinya syarat-syarat *sariqah hudūd*, pandangan mayoritas dan yang paling aplikatif adalah mengkualifikasikan pencurian aset digital sebagai *jarīmah ta'zīr*. Meskipun sanksi *hadd*-nya gugur karena *syubhat*, perbuatan mencuri itu sendiri tetap merupakan dosa besar dan tindak pidana yang harus dihukum. Dengan memasukkannya ke dalam kategori *ta'zīr*, hakim dan negara memiliki fleksibilitas untuk menjatuhkan hukuman yang berat dan proporsional, tanpa terikat pada syarat-syarat formalistik dari *sariqah hudūd*.

Pendekatan ini jauh lebih praktis dan efektif. Ia memungkinkan negara untuk membuat undang-undang pidana siber yang secara spesifik mengkriminalisasi berbagai bentuk peretasan dan pencurian data atau aset digital. Hukuman yang dijatuhkan bisa berupa penjara jangka panjang, denda yang sangat besar, dan perampasan aset, yang disesuaikan dengan skala dan dampak kejahatan. Ini sejalan dengan semangat hukum Islam yang bertujuan untuk melindungi harta (*ḥifẓ al-māl*) dan memberikan efek jera, meskipun melalui mekanisme sanksi yang berbeda.

Dengan demikian, seorang peretas yang mencuri jutaan dolar dalam bentuk *cryptocurrency* tidak akan lepas dari jerat hukum hanya karena perbuatannya tidak memenuhi syarat potong tangan. Sebaliknya, ia akan diadili berdasarkan undang-undang pidana siber (sebagai bentuk legislasi *ta'zīr*) dan dapat dijatuhi hukuman penjara puluhan tahun. Pendekatan ini menunjukkan bahwa hukum pidana Islam bukanlah sistem yang kaku, melainkan memiliki mekanisme internal (*ta'zīr*) untuk beradaptasi dengan bentuk-bentuk kejahatan baru yang tidak terbayangkan oleh para yuris klasik.

3. Konsep Hirabah (Perampokan) dalam Konteks Peretasan Skala Besar

Untuk kasus-kasus peretasan yang sangat besar dan terorganisir, seperti serangan oleh kelompok peretas yang disponsori negara terhadap bursa kripto atau infrastruktur keuangan digital suatu negara, sebagian ulama mencoba menganalogikannya dengan konsep *ḥirābah*. *Ḥirābah* adalah kejahatan perampokan atau pengacauan keamanan yang dilakukan dengan kekerasan atau ancaman secara terang-terangan, yang bertujuan untuk merampas harta, membunuh, atau meneror masyarakat. Sanksi untuk *ḥirābah* sangat berat dan ditetapkan dalam Al-Qur'an (Al-Ma'idah: 33), bisa berupa hukuman mati, salib, potong tangan dan kaki secara bersilang, atau diasingkan.

Analogi ini didasarkan pada dampak kejahatan tersebut. Peretasan skala besar yang menargetkan infrastruktur keuangan vital tidak hanya sekadar mencuri harta, tetapi juga mengganggu stabilitas ekonomi, merusak ketertiban umum, dan menyebarkan ketakutan di tengah masyarakat. Dampak destruktifnya dianggap setara dengan *mafsadah* (kerusakan) yang ditimbulkan oleh perampok di jalanan. Kelompok peretas seperti Lazarus Group, yang serangannya dimotivasi oleh tujuan politik dan ekonomi negara, dapat dipandang sebagai "perampok digital" yang mengancam keamanan siber global.

Namun, sama seperti pada *sariqah*, penerapan sanksi *hadd* untuk *ḥirābah* juga menghadapi perdebatan, terutama mengenai unsur "kekerasan atau ancaman fisik" yang menjadi ciri khasnya. Meskipun demikian, semangat di balik larangan *ḥirābah*—yaitu memberantas kejahatan terorganisir yang mengancam keamanan publik—sangat relevan. Bahkan jika sanksi *hadd*-nya tidak diterapkan, pengkualifikasian peretasan skala besar sebagai kejahatan yang setara dengan *ḥirābah* memberikan justifikasi untuk menjatuhkan hukuman *ta'zīr* yang paling berat, termasuk hukuman mati dalam kasus-kasus ekstrem yang mengancam keamanan negara, sesuai dengan kebijakan *siyāsah syar'iyyah* penguasa.

4. Hukuman Ta'zir untuk Pencurian yang Proporsional dengan Kerugian

Ketika pencurian aset digital dikategorikan sebagai *jarīmah ta'zīr*, salah satu prinsip utama dalam penjatuhan hukumannya adalah proporsionalitas. Hakim harus mempertimbangkan berbagai faktor untuk menentukan berat ringannya sanksi. Faktor-faktor ini meliputi jumlah kerugian finansial yang diderita korban, tingkat kecanggihan serangan, apakah pelaku adalah residivis, dan apakah serangan tersebut menargetkan individu yang rentan atau infrastruktur penting. Hukuman untuk peretas profesional yang mencuri jutaan dolar tentu harus lebih berat daripada hukuman untuk pelaku pemula yang mencuri dalam jumlah kecil.

Selain hukuman yang bersifat punitif seperti penjara dan denda, hukuman *ta'zīr* juga harus berorientasi pada pemulihan. Prioritas utama adalah mengembalikan aset yang dicuri kepada pemiliknya yang sah. Oleh karena itu, bagian tak terpisahkan dari proses hukum adalah pelacakan aset (*asset tracing*) dan perampasan aset (*asset recovery*). Negara harus mengerahkan kemampuannya untuk menyita aset kripto yang ada di dompet pelaku atau hasil kejahatan lain yang dibeli menggunakan dana curian, untuk kemudian direstitusikan kepada para korban.

Prinsip proporsionalitas dan keadilan ini memastikan bahwa sistem peradilan tidak hanya fokus pada penghukuman, tetapi juga pada pemulihan hak-hak korban dan perbaikan kerusakan yang telah terjadi. Fleksibilitas hukuman *ta'zīr* memungkinkan hakim untuk merancang sebuah putusan yang komprehensif, yang memberikan efek jera pada pelaku, memberikan keadilan bagi korban, dan mengirimkan pesan yang kuat kepada masyarakat tentang keseriusan negara dalam memberantas kejahatan siber, semuanya dalam koridor yang sejalan dengan tujuan luhur syariah (*Maqāshid al-Sharī'ah*).

C. Pencucian Uang sebagai Kejahatan Terorganisir (*Ṫanzhim Ijrami*)

Pencucian uang adalah kejahatan sekunder yang bertujuan menyembunyikan atau menyamarkan hasil dari kejahatan primer. Dalam hukum Islam, meskipun tidak ada istilah tunggal untuk "pencucian uang",

esensi perbuatannya secara tegas dilarang melalui berbagai prinsip. Sub-bab ini akan mengkualifikasikan pencucian uang sebagai kejahatan terorganisir, mengaitkannya dengan larangan menyembunyikan harta haram dan membantu perbuatan maksiat, serta membahas sanksi dan peran negara dalam merampas aset hasil kejahatan.

1. Larangan Menyembunyikan Harta Hasil Kejahatan

Hukum Islam sangat menekankan bahwa harta harus diperoleh melalui cara-cara yang halal (*ṭayyib*). Harta yang diperoleh dari sumber haram—seperti pencurian, korupsi, penipuan, atau penjualan barang terlarang—adalah harta yang tidak memiliki keberkahan dan status kepemilikannya batal. Seseorang yang memiliki harta haram berkewajiban untuk membersihkan dirinya dengan mengembalikan harta tersebut kepada pemiliknya yang sah, atau jika tidak memungkinkan, menyedekahkannya atas nama pemiliknya. Menggunakan, menikmati, atau menyembunyikan harta hasil kejahatan adalah perbuatan dosa yang berkelanjutan.

Pencucian uang, pada intinya, adalah upaya sistematis untuk menyembunyikan status haram dari sebuah harta dan membuatnya tampak halal. Perbuatan ini secara langsung bertentangan dengan prinsip kejujuran dan keadilan dalam Islam. Ia dapat dikualifikasikan sebagai bentuk konspirasi untuk melanggengkan kezaliman dan melindungi pelaku kejahatan dari pertanggungjawaban. Dengan demikian, meskipun tidak disebutkan secara eksplisit dalam teks-teks klasik, perbuatan menyamarkan asal-usul harta haram dapat dikategorikan sebagai *jarīmah ta'zīr* karena ia melanggar prinsip-prinsip fundamental syariah.

Larangan ini juga didasarkan pada prinsip "*ta'āwanū 'ala al-birri wa al-taqwā wa lā ta'āwanū 'ala al-ithmi wa al-'udwān*" (Tolong-menolonglah kamu dalam (mengerjakan) kebajikan dan takwa, dan jangan tolong-menolong dalam berbuat dosa dan pelanggaran) (Al-Ma'idah: 2). Pelaku pencucian uang, baik pelaku utama maupun pihak ketiga yang membantunya, secara aktif telah "tolong-menolong dalam berbuat dosa" dengan membantu para penjahat untuk menikmati hasil kejahatan mereka. Ini menjadikan perbuatan mereka sebagai tindak pidana yang berdiri sendiri.

2. Kategori sebagai Tindakan Membantu Kejahatan (I'anah 'ala al-Ma'siyah)

Dari perspektif partisipasi dalam tindak pidana (*al-ishtirāk fī al-jarīmah*), pelaku pencucian uang dapat dikategorikan sebagai orang yang membantu terjadinya atau keberlangsungan kejahatan (*i'ānah 'alā al-ma'ṣiyah*). Tanpa adanya mekanisme pencucian uang, banyak kejahatan primer (seperti perdagangan narkotika skala besar atau korupsi) akan menjadi kurang menarik, karena pelakunya akan kesulitan menggunakan hasil kejahatannya. Dengan menyediakan "jasa" untuk membersihkan uang haram, para pelaku pencucian uang secara efektif memberikan insentif dan memfasilitasi keberlangsungan kejahatan-kejahatan lainnya.

Dalam fikih jinayah, orang yang membantu terjadinya kejahatan, meskipun tidak secara langsung melakukan kejahatan primer, tetap dapat dimintai pertanggungjawaban pidana. Statusnya mungkin berbeda dari pelaku utama (*fā'il aṣlī*), tetapi ia tetap dapat dijatuhi hukuman *ta'zīr* yang berat. Hukuman ini dijatuhkan karena perannya dalam memungkinkan atau mempermudah terjadinya kerusakan (*mafsadah*) yang lebih besar di tengah masyarakat.

Dalam konteks modern, di mana pencucian uang sering kali dilakukan oleh sindikat profesional yang terorganisir (*tanẓīm ijrāmī*), tingkat pertanggungjawabannya menjadi semakin besar. Mereka bukan sekadar pembantu pasif, melainkan bagian integral dari infrastruktur kejahatan global. Oleh karena itu, hukuman yang dijatuhkan kepada mereka harus mencerminkan peran sentral mereka dalam ekosistem kriminal. Mengkriminalisasi pencucian uang adalah langkah krusial untuk memotong urat nadi finansial dari berbagai organisasi kejahatan.

3. Hukuman Ta'zir yang Berat untuk Memberi Efek Jera

Mengingat sifat pencucian uang sebagai kejahatan yang menjadi "pelumas" bagi kejahatan-kejahatan lain, sanksi yang dijatuhkan haruslah bersifat berat dan memberikan efek jera yang kuat. Sebagai *jarīmah ta'zīr*, hakim memiliki wewenang untuk menetapkan hukuman yang melampaui sanksi untuk kejahatan harta biasa. Hukuman penjara jangka panjang adalah sanksi yang paling umum dan relevan, yang durasinya harus sepadan dengan jumlah uang yang dicuci dan tingkat kecanggihan operasinya.

Selain penjara, denda finansial yang sangat besar juga merupakan hukuman yang efektif. Denda ini idealnya harus melebihi jumlah uang yang berhasil dicuci, untuk memastikan bahwa "kejahatan tidak menghasilkan keuntungan" (*crime does not pay*). Tujuan dari denda yang memberatkan ini adalah untuk membuat kalkulasi biaya-manfaat dari kegiatan pencucian uang menjadi tidak menarik bagi para calon pelaku.

Dalam kasus-kasus di mana pencucian uang terkait dengan kejahatan yang mengancam keamanan negara, seperti pendanaan terorisme atau perdagangan senjata, hukuman *ta'zīr* yang dijatuhkan bisa mencapai tingkat yang paling berat, sesuai dengan kebijakan penguasa untuk menjaga ketertiban umum. Beratnya sanksi ini mengirimkan pesan yang jelas bahwa negara dan sistem hukum Islam tidak akan menoleransi upaya-upaya untuk merusak integritas sistem keuangan dan memfasilitasi kejahatan terorganisir.

4. Kewajiban Negara untuk Merampas Aset Hasil Kejahatan

Salah satu aspek terpenting dalam penanganan kasus pencucian uang dari perspektif hukum Islam adalah perampasan aset. Harta yang telah terbukti berasal dari sumber yang haram atau merupakan hasil dari proses pencucian uang harus disita oleh negara. Prinsip dasarnya adalah bahwa kepemilikan atas harta haram adalah batal, dan harta tersebut harus dikembalikan kepada sumbernya yang sah. Jika pemilik aslinya (misalnya, korban penipuan) dapat diidentifikasi, maka aset tersebut wajib dikembalikan kepada mereka.

Jika pemilik asli tidak dapat diidentifikasi (misalnya, dalam kasus perdagangan narkotika), maka aset yang dirampas tersebut menjadi milik kas negara (*bayt al-māl*) untuk digunakan demi kemaslahatan umum. Dana ini dapat digunakan untuk membiayai program-program sosial, membangun infrastruktur, atau memperkuat lembaga penegak hukum itu sendiri. Perampasan aset ini bukan hanya berfungsi sebagai hukuman tambahan bagi pelaku, tetapi juga sebagai cara untuk memulihkan kerusakan sosial yang ditimbulkan oleh kejahatan mereka.

Kewajiban negara untuk secara aktif melacak, membekukan, dan merampas aset hasil kejahatan adalah implementasi dari prinsip *ḥifẓ al-māl* dalam skala makro. Ini memastikan bahwa sistem ekonomi tidak dicemari

oleh uang haram dan bahwa para penjahat tidak dapat menikmati buah dari kejahatan mereka. Dalam konteks *cryptocurrency*, ini berarti negara harus memiliki kapasitas teknis untuk melacak aset digital lintas *blockchain* dan bekerja sama dengan negara lain untuk menyita aset yang disimpan di luar negeri.

D. Pendanaan Terorisme sebagai Hirabah atau Bughat

Pendanaan terorisme adalah salah satu kejahatan paling serius karena dampaknya yang mengancam nyawa manusia dan stabilitas negara. Hukum pidana Islam memiliki kategori-kategori khusus untuk kejahatan yang mengganggu keamanan publik dalam skala besar. Sub-bab ini akan menganalisis bagaimana pendanaan terorisme dapat dikualifikasikan di bawah konsep *ḥirābah* (terorisme dan pengacauan keamanan) atau *bughāt* (pemberontakan), serta membahas ketegasan sanksi dan pentingnya prinsip pencegahan.

1. Analisis Pendanaan Terorisme sebagai Tindakan Merusak Keamanan (Hirabah)

Konsep *ḥirābah*, seperti yang telah disinggung sebelumnya, merujuk pada tindakan kekerasan atau teror yang dilakukan oleh individu atau kelompok untuk merampas harta, membunuh, atau menciptakan ketakutan dan kekacauan di tengah masyarakat. Aksi terorisme modern, seperti pengeboman di tempat umum atau serangan terhadap warga sipil, adalah manifestasi sempurna dari kejahatan *ḥirābah*. Para pelakunya sering disebut sebagai *muḥāribūn* (orang-orang yang memerangi Allah dan Rasul-Nya) atau *mufsidūn fī al-arḍ* (perusak di muka bumi).

Pendanaan terorisme, meskipun tidak secara langsung melakukan aksi kekerasan, merupakan bagian yang tidak terpisahkan dari kejahatan *ḥirābah*. Tanpa dana, kelompok teroris tidak dapat membeli senjata, bahan peledak, atau membiayai operasi mereka. Oleh karena itu, orang yang mendanai terorisme dapat dianggap sebagai peserta atau pembantu (*accomplice*) dalam kejahatan *ḥirābah*. Peran mereka dianalogikan seperti orang yang menyediakan senjata atau kendaraan bagi para perampok. Dalam hukum Islam, pembantu dalam kejahatan serius dapat dijatuhi hukuman *ta'zīr* yang berat, yang dalam kasus ini bisa mendekati beratnya hukuman bagi pelaku utama.

Dengan mengkualifikasikan pendanaan terorisme sebagai bagian dari *jarīmah ḥirābah*, hukum Islam memberikan landasan yang sangat kuat untuk menindaknya dengan sangat keras. Ini bukan lagi sekadar kejahatan finansial biasa, melainkan sebuah kejahatan terhadap keamanan publik dan negara. Setiap sen yang disumbangkan untuk tujuan terorisme, baik melalui *cryptocurrency* maupun cara lain, adalah kontribusi terhadap aksi perusakan dan pertumpahan darah yang dilarang keras oleh syariah.

2. Analisis sebagai Pemberontakan (Bughat) jika Bertujuan Menggulingkan Pemerintahan Sah

Jika tujuan dari kelompok teroris tersebut secara spesifik adalah untuk menggulingkan pemerintahan yang sah (*imām* atau *ulil amri*) melalui kekuatan bersenjata, maka tindakan mereka dan para pendukungnya dapat dikualifikasikan di bawah kategori *bughāt* (pemberontakan). *Bughāt* adalah kejahatan politik yang sangat serius, di mana sekelompok orang dengan kekuatan dan interpretasi (takwil) tertentu memberontak terhadap pemimpin yang legitimate. Hukum Islam memberikan hak kepada negara untuk memerangi para pemberontak demi menjaga integritas dan stabilitas negara.

Pendanaan untuk kelompok pemberontak dianggap sebagai tindakan mendukung *bughāt* dan merupakan tindak pidana yang serius. Negara berhak untuk memutus semua aliran dana kepada kelompok tersebut dan menghukum siapa saja yang terbukti memberikan dukungan finansial. Perbedaan utama antara *ḥirābah* dan *bughāt* terletak pada tujuannya; *ḥirābah* lebih bersifat kriminal murni (meneror dan merampok), sementara *bughāt* memiliki tujuan politik untuk merebut kekuasaan. Namun, dalam banyak kasus terorisme modern, kedua unsur ini sering kali tumpang tindih.

Pengkualifikasian sebagai *bughāt* memberikan legitimasi penuh kepada negara untuk menggunakan kekuatan militer dan hukum untuk menumpas gerakan tersebut. Dari perspektif hukum pidana, para pendukung finansial dari gerakan pemberontakan dapat diadili atas kejahatan makar dan dijatuhi hukuman *ta'zīr* yang sangat berat, yang bisa mencakup hukuman mati, tergantung pada tingkat keterlibatan dan dampak yang ditimbulkan. Ini menunjukkan bahwa hukum Islam tidak memberikan toleransi terhadap upaya-upaya yang dapat menyebabkan perang saudara dan anarki.

3. Sanksi Tegas dalam Islam terhadap Terorisme dan Pendukungnya

Baik dikualifikasikan sebagai *ḥirābah* maupun *bughāt*, hukum Islam menetapkan sanksi yang sangat tegas terhadap terorisme dan semua bentuk dukungannya. Untuk pelaku utama *ḥirābah*, Al-Qur'an surat Al-Ma'idah ayat 33 telah menggariskan sanksi *hadd* yang berat. Bagi para pendukung, termasuk pendana, sanksi *ta'zīr* yang dijatuhkan haruslah mencerminkan keseriusan kejahatan tersebut. Hukuman penjara seumur hidup atau bahkan hukuman mati dapat dibenarkan dari perspektif *siyāsah syar'iyyah* (kebijakan pemerintahan yang sesuai syariah) untuk melindungi masyarakat dari bahaya yang lebih besar.

Tujuan dari sanksi yang tegas ini adalah untuk memberikan efek jera maksimal (*general deterrence*) dan untuk melumpuhkan jaringan teroris secara total. Tidak ada ruang untuk keringanan hukuman bagi mereka yang terbukti secara sadar mendanai aktivitas yang menyebabkan hilangnya nyawa orang-orang yang tidak bersalah. Sikap tanpa kompromi ini sejalan dengan salah satu tujuan utama syariah, yaitu perlindungan terhadap jiwa (*ḥifẓ al-nafs*), yang merupakan salah satu dari lima nilai universal yang paling fundamental.

Selain sanksi pidana, para pendukung terorisme juga harus menghadapi sanksi sosial, yaitu dengan mengutuk perbuatan mereka dan mengisolasi ideologi mereka dari masyarakat. Para ulama dan pemimpin masyarakat memiliki peran penting dalam melakukan kontra-narasi terhadap propaganda teroris yang sering kali menyalahgunakan ayat-ayat Al-Qur'an dan Hadis untuk membenarkan tindakan keji mereka.

4. Prinsip Pencegahan (Sadd al-Dzari'ah) untuk Memutus Aliran Dana

Selain penindakan, hukum Islam juga sangat menekankan aspek pencegahan, yang terangkum dalam prinsip *sadd al-żarī'ah* (menutup jalan atau sarana yang menuju kepada keburukan). Dalam konteks pendanaan terorisme, prinsip ini menuntut negara untuk secara proaktif menutup semua celah dan sarana yang dapat digunakan oleh teroris untuk menggalang dan memindahkan dana. Ini memberikan landasan syariah yang kuat bagi pemerintah untuk memberlakukan regulasi yang ketat terhadap sistem keuangan.

Implementasi prinsip ini dalam konteks *cryptocurrency* berarti mewajibkan semua penyedia layanan aset virtual (seperti bursa kripto) untuk menerapkan prosedur *Know Your Customer* (KYC) dan *Anti-Money Laundering* (AML) yang ketat. Bursa harus memverifikasi identitas penggunanya, memantau transaksi secara *real-time* untuk mendeteksi pola yang mencurigakan (misalnya, transaksi ke alamat yang masuk daftar hitam), dan segera melaporkannya kepada pihak berwenang seperti PPATK atau Densus 88.

Tindakan-tindakan seperti memblokir akses ke situs web yang mempromosikan donasi teroris, membekukan aset kripto yang teridentifikasi terkait dengan terorisme, dan melakukan pengawasan ketat terhadap platform P2P adalah bentuk konkret dari *sadd al-żarī'ah*. Meskipun beberapa tindakan ini mungkin membatasi privasi atau kebebasan transaksi, kemaslahatan yang lebih besar—yaitu mencegah terjadinya aksi terorisme dan melindungi nyawa manusia—jauh lebih diutamakan. Prinsip ini membenarkan tindakan preventif negara demi menolak kerusakan (*dar' al-mafāsid*) yang jauh lebih besar.

E. Perdagangan Ilegal sebagai Jarimah Ta'zir

Pasar gelap di *dark web* yang difasilitasi oleh *cryptocurrency* adalah pusat perdagangan barang dan jasa yang secara inheren dilarang oleh hukum Islam dan hukum positif. Sub-bab ini akan menganalisis bagaimana partisipasi dalam pasar gelap ini, baik sebagai penjual, pembeli, maupun penyedia platform, dikualifikasikan sebagai tindak pidana *ta'zīr*. Pembahasan akan mencakup larangan memperjualbelikan barang haram, statusnya sebagai kejahatan yang merusak tatanan sosial, dan pertanggungjawaban pidana bagi para pihak yang terlibat.

1. Larangan Memperjualbelikan Barang Haram (Narkotika, dll.)

Hukum Islam secara tegas melarang produksi, konsumsi, dan perdagangan barang-barang yang dianggap haram dan berbahaya (*ḍarar*). Kategori ini mencakup narkotika dan zat memabukkan lainnya (dianalogikan dengan *khamr*), senjata yang dijual untuk tujuan kriminal, data curian (karena merupakan harta hasil kejahatan), dan layanan ilegal lainnya. Prinsip dasarnya adalah hadis Nabi Muhammad SAW yang

menyatakan, "Sesungguhnya Allah jika mengharamkan sesuatu, maka Dia juga mengharamkan harganya (hasil penjualannya)." (HR. Abu Dawud).

Oleh karena itu, setiap transaksi jual beli yang terjadi di pasar gelap *dark web* untuk barang-barang tersebut adalah akad yang batal (*bāṭil*) dan perbuatan yang haram. Para pelakunya, baik penjual maupun pembeli, telah melakukan tindak pidana *ta'zīr*. Penjual melakukan kejahatan karena memperdagangkan barang terlarang, sementara pembeli melakukan kejahatan karena mengonsumsi atau menggunakan barang tersebut dan karena membelanjakan hartanya untuk kemaksiatan. Penggunaan *cryptocurrency* sebagai alat bayar tidak mengubah status haram dari transaksi itu sendiri.

Negara, sebagai *ulil amri*, memiliki kewajiban untuk melarang dan memberantas perdagangan ini dengan segala cara. Undang-undang tentang narkotika, senjata api, atau kejahatan siber yang melarang perdagangan barang-barang ini adalah bentuk legislasi *ta'zīr* yang sah dan wajib ditegakkan. Penegakan hukum terhadap para pelaku di pasar gelap adalah implementasi langsung dari kewajiban negara untuk menegakkan syariah dan melindungi masyarakat dari bahaya.

2. Kualifikasi sebagai Kejahatan yang Merusak Masyarakat (Mufsid fil-Ardh)

Perdagangan ilegal di *dark web* bukan sekadar kumpulan transaksi haram individual, melainkan sebuah ekosistem kejahatan terorganisir yang memiliki dampak merusak (*mafsadah*) yang sangat luas bagi masyarakat. Perdagangan narkotika merusak kesehatan fisik dan mental generasi muda (*ḥifẓ al-nafs* dan *ḥifẓ al-'aql*). Perdagangan data curian merusak privasi dan keamanan finansial individu (*ḥifẓ al-māl*). Perdagangan senjata memfasilitasi kekerasan dan kejahatan lainnya. Secara kolektif, aktivitas pasar gelap ini menggerogoti fondasi moral dan keamanan masyarakat.

Karena dampaknya yang sistemik ini, para pelaku utama di balik pasar gelap—seperti operator platform, administrator, dan penjual skala besar—dapat dikualifikasikan sebagai *mufsid fī al-arḍ* (perusak di muka bumi). Istilah ini digunakan dalam Al-Qur'an untuk menggambarkan para penjahat yang perbuatannya menyebabkan kerusakan dan kekacauan yang luas.

Kualifikasi ini menempatkan kejahatan mereka pada tingkat keseriusan yang sangat tinggi, setara dengan kejahatan *ḥirābah*.

Dengan status sebagai *mufsid fī al-arḍ*, mereka layak dijatuhi hukuman *ta'zīr* yang paling berat. Hukuman tersebut harus mampu merefleksikan skala kerusakan sosial yang mereka timbulkan. Tujuannya bukan hanya untuk menghukum perbuatan mereka, tetapi juga untuk membersihkan masyarakat dari pengaruh destruktif mereka dan mencegah munculnya platform-platform serupa di masa depan. Ini adalah bentuk perlindungan negara terhadap lima nilai universal (*al-ḍarūriyyāt al-khamsah*) dari ancaman kejahatan terorganisir.

3. Tanggung Jawab Pidana bagi Penyedia Platform dan Pengguna

Dalam ekosistem pasar gelap, pertanggungjawaban pidana tidak hanya terbatas pada penjual dan pembeli. Para pihak yang secara sadar menciptakan dan mengelola infrastruktur yang memungkinkan terjadinya kejahatan ini juga harus dimintai pertanggungjawaban. Ini termasuk para administrator platform, pemrogram yang merancang situs, dan penyedia layanan hosting yang mengetahui bahwa server mereka digunakan untuk tujuan ilegal. Peran mereka adalah sebagai fasilitator utama, yang tanpanya pasar tersebut tidak akan ada.

Berdasarkan prinsip *i'ānah 'alā al-ma'ṣiyah* (membantu dalam kemaksiatan), para penyedia platform ini adalah kaki tangan utama dalam setiap transaksi ilegal yang terjadi. Mereka mengambil keuntungan (biasanya dalam bentuk komisi dari setiap transaksi) dari aktivitas kriminal. Oleh karena itu, hukuman mereka harus setara atau bahkan lebih berat daripada para penjual individual. Kasus penangkapan Ross Ulbricht, pendiri Silk Road, yang dijatuhi hukuman penjara seumur hidup oleh pengadilan AS, mencerminkan logika ini.

Pengguna atau pembeli juga tidak lepas dari tanggung jawab pidana, meskipun tingkat kesalahannya mungkin lebih rendah daripada penjual atau operator platform. Dengan membeli barang ilegal, mereka menciptakan permintaan yang menjadi bahan bakar bagi keberlangsungan pasar gelap. Mereka dapat dituntut atas kejahatan kepemilikan barang ilegal (misalnya,

kepemilikan narkotika) dan dijatuhi hukuman *ta'zīr* yang sesuai, seperti rehabilitasi, denda, atau penjara singkat, tergantung pada kebijakan hukum negara dan tingkat keterlibatan mereka.

4. Hukuman Ta'zir untuk Perdagangan Ilegal di Dunia Maya

Sebagaimana kejahatan *ta'zīr* lainnya, hukuman untuk perdagangan ilegal di dunia maya harus bersifat fleksibel dan multifaset. Untuk para operator dan penjual skala besar, hukuman penjara jangka panjang hingga seumur hidup adalah sanksi yang proporsional. Hukuman ini mencerminkan peran sentral mereka dalam menciptakan dan memelihara ekosistem kejahatan yang merusak masyarakat secara luas.

Selain hukuman badan, perampasan seluruh aset yang terkait dengan aktivitas ilegal adalah suatu keharusan. Ini termasuk menyita semua *cryptocurrency* yang ada di akun *escrow* platform, keuntungan yang diperoleh operator, dan aset lain yang dibeli menggunakan hasil kejahatan. Langkah ini penting untuk memastikan bahwa kejahatan tidak memberikan keuntungan finansial sama sekali dan untuk melumpuhkan kapasitas ekonomi para pelaku.

Untuk pembeli atau pengguna tingkat rendah, pendekatan hukuman dapat lebih berorientasi pada rehabilitasi, terutama dalam kasus penyalahgunaan narkotika. Namun, penegakan hukum yang konsisten terhadap pembeli juga penting untuk mengurangi permintaan. Kombinasi dari penindakan keras terhadap para bandar dan operator, serta upaya untuk mengurangi permintaan dari sisi konsumen, merupakan strategi komprehensif yang sejalan dengan pendekatan hukum Islam dalam memberantas kejahatan dari akarnya.

Analisis Mendalam Konsep Kunci Bab 5: Kualifikasi Fikih Jinayah untuk Kejahatan Kripto

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk membuktikan bahwa hukum pidana Islam bukanlah sistem yang usang, melainkan memiliki mekanisme internal untuk beradaptasi dan memberikan status hukum (*hukm*) terhadap kejahatan-kejahatan kontemporer. Tujuannya adalah untuk:

1. Memberikan Kerangka Analisis Syar'i: Menyediakan metode untuk "menerjemahkan" kejahatan digital ke dalam bahasa fikih jinayah.
2. Menentukan Kategori Pidana: Mengkualifikasikan setiap modus operandi kejahatan kripto ke dalam kategori *jarimah* yang tepat (yang hampir seluruhnya akan jatuh ke dalam *Ta'zir*).
3. Menjustifikasi Penindakan: Memberikan landasan teologis dan yuridis Islam bagi negara untuk menindak para pelaku kejahatan ini.
4. Mengeksplorasi Sanksi: Membuka diskusi tentang jenis sanksi berbasis *Ta'zir* yang adil, proporsional, dan efektif untuk setiap jenis kejahatan.

Ini adalah proses intelektual di mana esensi perbuatan modern dicari padanannya dalam prinsip-prinsip hukum Islam klasik.

Elemen-Elemen Kunci dalam Proses Kualifikasi:

1. Analisis Esensi Perbuatan (*Manāṭ al-Hukm*): Apa inti dari perbuatan tersebut, terlepas dari medium teknologinya? Apakah itu penipuan, pencurian, perusakan, atau membantu kejahatan?
2. Pencarian Dalil atau Prinsip Umum: Adakah ayat Al-Qur'an, Hadis, atau kaidah fikih umum yang melarang esensi perbuatan tersebut? (Contoh: Larangan memakan harta secara batil, larangan tolong-menolong dalam dosa).
3. Proses Analogi (*Qiyas*): Menganalogikan kejahatan modern dengan kejahatan serupa yang sudah dikenal dalam fikih klasik.
4. Penentuan Kategori Jarimah: Memutuskan apakah perbuatan tersebut masuk kategori *Hudud, Qisas*, atau (yang paling mungkin) *Ta'zir*.

Analisis Komparatif: Kualifikasi Fikih untuk Setiap Modus Operandi

Tabel berikut memetakan proses kualifikasi untuk setiap jenis kejahatan kripto yang telah diidentifikasi di Bab 4.

Modus Operandi (dari Bab 4)	Esensi Perbuatan	Prinsip Umum yang Dilanggar	Analogi Fikih Klasik	Kualifikasi Jarimah (Hasil Akhir)
Penipuan Investasi Kripto (*Scam*)	Mengambil harta orang lain dengan tipu muslihat dan janji palsu.	Larangan memakan harta secara batil (QS. An-Nisa: 29). Unsur *Gharar* (ketidakpastian) & *Tadlis* (penipuan).	Penipuan di pasar (*ghish*), jual beli yang mengandung tipuan.	Jarimah Ta'zir. Sanksi ditentukan oleh hakim untuk memberi efek jera dan mengembalikan kerugian.
Pencurian Aset Digital (*Hacking*)	Mengambil harta dari tempat simpannya secara diam-diam tanpa hak.	Larangan mencuri (QS. Al-Maidah: 38). Kewajiban menjaga harta (*Hifzh al-Maal*).	Pencurian (*Sariqah*). Namun, diperdebatkan apakah memenuhi syarat *hudud*.	Sariqah Ta'ziriyah. Dianggap pencurian, namun sanksinya fleksibel (*ta'zir*) karena tidak memenuhi syarat *hirz* (tempat simpan) fisik untuk *hudud*.
Pencucian Uang (*Money Laundering*)	Membantu menyembunyikan dan menyamarkan asal-usul harta hasil kejahatan.	Larangan tolong-menolong dalam dosa dan permusuhan (QS. Al-Maidah: 2).	*I'anah 'ala al-Ma'siyah* (membantu dalam kemaksiatan).	Jarimah Ta'zir. Dianggap kejahatan terorganisir (*tanzhim ijrami*) yang sanksinya bisa sangat berat.
Pendanaan Terorisme	Menyediakan dana untuk kegiatan yang menyebarkan teror dan merusak keamanan publik.	Larangan membunuh jiwa tanpa hak (QS. Al-Isra: 33). Larangan berbuat kerusakan di muka bumi (*ifsad fil-ardh*).	Perampokan bersenjata (*Hirabah*) atau Pemberontakan (*Bughat*), karena sama-sama mengancam keamanan negara.	Jarimah Hirabah atau Bughat. Keduanya merupakan kejahatan berat dengan sanksi yang telah ditetapkan *nash* atau sanksi *ta'zir* yang sangat tegas.
Transaksi Ilegal di Dark Web	Memperjualbelikan barang/jasa yang secara zat diharamkan (narkotika, data curian).	Larangan jual beli barang haram. Larangan merusak akal (*hifzh al-'aql*) dan jiwa (*hifzh al-nafs*).	Jual beli barang terlarang (*bay' al-haram*).	Jarimah Ta'zir. Dapat dikategorikan sebagai *ifsad fil-ardh* (perusakan di muka bumi) jika dampaknya masif.

Kontribusi Konsep Kualifikasi Fikih dalam Bab 5:

Konsep ini adalah puncak dari analisis teoretis hukum pidana Islam dalam buku ini.

1. Menjawab Pertanyaan Sentral: Bab ini secara langsung menjawab pertanyaan, "Bagaimana hukum pidana Islam memandang dan menghukum kejahatan kripto?" Jawabannya adalah melalui pintu *Ta'zir* yang luas.
2. Membangun Jembatan Intelektual: Proses kualifikasi ini menunjukkan bagaimana para ahli hukum Islam (*fuqaha*) dapat melakukan *ijtihad* untuk menjaga relevansi syariah. Ini adalah contoh nyata dari dinamisme hukum Islam.
3. Memberikan Landasan untuk Rekomendasi: Dengan berhasil mengkualifikasikan setiap kejahatan, Bab 5 membuka jalan untuk Bab 9 (Analisis Kasus) dan Bab 12 (Strategi Represif). Rekomendasi sanksi yang fleksibel, fokus pada ganti rugi, dan penggunaan sanksi publikasi, semuanya berasal dari pemahaman mendalam tentang konsep *Ta'zir* yang dieksplorasi di bab ini.

Secara ringkas, Bab 5 adalah "ruang sidang" fikih. Ia mengambil "berkas perkara" (modus operandi dari Bab 4) dan "undang-undang" (prinsip fikih jinayah dari Bab 2), lalu seorang "hakim" (penulis) melakukan analisis untuk menjatuhkan "vonis" kualifikasi hukum. Hasilnya adalah sebuah justifikasi yang kuat bahwa hukum pidana Islam tidak gagap teknologi dan memiliki perangkat yang memadai untuk menghadapi kejahatan di era digital.

BAB 6

Analisis Hukum Positif Indonesia Terkait Kejahatan Ekonomi Digital

Setelah Bab 5 mengkualifikasikan kejahatan *cryptocurrency* dari perspektif hukum pidana Islam, Bab 6 mengalihkan fokus pada kerangka hukum positif yang berlaku di Negara Kesatuan Republik Indonesia. Dalam sebuah negara hukum, penindakan terhadap setiap tindak pidana harus memiliki landasan yuridis-formal yang jelas dalam peraturan perundang-undangan yang berlaku. Analisis terhadap hukum positif ini penting untuk memahami bagaimana negara secara konkret merespons kejahatan ekonomi digital, serta untuk melihat titik-titik persinggungan dan potensi harmonisasi dengan prinsip-prinsip hukum pidana Islam. *Research gap* yang diisi oleh bab ini adalah kurangnya pembahasan yang mengintegrasikan analisis terhadap berbagai instrumen hukum yang relevan—dari KUHP, UU ITE, UU TPPU, hingga regulasi sektoral Bappebti—dalam satu narasi yang koheren untuk melihat arsitektur penegakan hukum kejahatan kripto di Indonesia secara holistik. Pertanyaan penelitian utama yang akan dijawab adalah: Sejauh mana perangkat hukum positif Indonesia saat ini mampu menjangkau dan memberantas berbagai modus operandi kejahatan ekonomi digital yang menggunakan *cryptocurrency*, dan apa saja tantangan utama dalam implementasinya?

A. Kitab Undang-Undang Hukum Pidana (KUHP)

Kitab Undang-Undang Hukum Pidana (KUHP) merupakan induk dari hukum pidana di Indonesia. Meskipun disusun jauh sebelum era digital, beberapa pasalnya yang bersifat umum masih memiliki relevansi untuk menjerat kejahatan konvensional yang dilakukan dengan modus baru. Sub-bab ini akan menganalisis penerapan pasal-pasal penipuan dan penggelapan dalam KUHP terhadap kasus kejahatan kripto, sekaligus menyoroti keterbatasan inheren dari KUHP dan arah pembaharuannya dalam menghadapi tantangan kejahatan siber.

1. Penerapan Pasal Penipuan (Pasal 378 KUHP)

Pasal 378 KUHP tentang penipuan (*oplichting*) menjadi salah satu pasal yang paling sering digunakan untuk menjerat pelaku investasi bodong, termasuk yang berkedok *cryptocurrency*. Unsur-unsur dalam pasal ini adalah: (1) dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum; (2) memakai nama palsu atau martabat palsu,

dengan tipu muslihat, ataupun rangkaian kebohongan; (3) menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang. Unsur-unsur ini sangat relevan dengan skema penipuan kripto.

Dalam kasus skema Ponzi atau piramida kripto, pelaku menggunakan "rangkaian kebohongan" dengan menjanjikan keuntungan tidak realistis melalui "robot trading" atau "teknologi canggih". Tipu muslihat ini "menggerakkan" korban untuk "menyerahkan barang sesuatu", yang dalam hal ini adalah uang atau aset kripto mereka. Meskipun aset kripto tidak berwujud, dalam penafsiran hukum modern, ia diakui sebagai "barang" dalam pengertian hukum, khususnya sebagai benda tidak berwujud yang memiliki nilai ekonomis. Dengan demikian, Pasal 378 KUHP tetap dapat menjadi dasar hukum yang kuat untuk menuntut para pelaku penipuan investasi kripto.

Tantangan dalam penerapannya sering kali terletak pada pembuktian unsur "tipu muslihat" atau "rangkaian kebohongan" dalam ranah digital yang kompleks dan anonim. Penegak hukum harus mampu menyajikan bukti digital yang menunjukkan adanya niat jahat dari pelaku sejak awal, bukan sekadar kegagalan bisnis yang wajar. Meskipun demikian, pasal ini tetap menjadi fondasi awal dalam penanganan hukum terhadap penipuan berbasis kripto sebelum menggunakan undang-undang yang lebih spesifik.

2. Penerapan Pasal Penggelapan (Pasal 372 KUHP)

Pasal 372 KUHP tentang penggelapan juga dapat diterapkan dalam beberapa skenario kejahatan kripto. Unsur utama penggelapan adalah "dengan sengaja dan melawan hukum memiliki barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, tetapi yang ada dalam kekuasaannya bukan karena kejahatan". Perbedaan kunci dengan pencurian adalah bahwa pada saat barang diserahkan, penguasaan atas barang tersebut terjadi secara sah (misalnya, karena dititipkan atau dipercayakan), namun kemudian pelaku menyalahgunakan kepercayaan tersebut.

Pasal ini relevan untuk kasus di mana seorang manajer investasi kripto atau pengelola platform *staking* melarikan diri dengan dana nasabah. Para nasabah secara sukarela "menyerahkan" atau "mempercayakan" aset kripto mereka kepada pengelola untuk diinvestasikan. Penguasaan aset oleh pengelola pada awalnya sah berdasarkan perjanjian. Namun, ketika pengelola tersebut secara diam-diam mentransfer aset nasabah ke dompet pribadinya dan menghilang (*exit scam*), ia telah melakukan penggelapan. Ia memiliki aset yang bukan miliknya, yang berada dalam kekuasaannya secara sah pada awalnya.

Sama seperti pasal penipuan, pembuktian dalam kasus penggelapan digital memerlukan analisis jejak transaksi di *blockchain* untuk menunjukkan aliran dana dari dompet kustodian (penitipan) ke dompet pribadi pelaku. Pasal ini memberikan kerangka hukum untuk kasus-kasus penyalahgunaan kepercayaan dalam industri jasa keuangan kripto, melengkapi pasal penipuan yang lebih fokus pada tipu muslihat di awal transaksi.

3. Keterbatasan KUHP dalam Menjangkau Kejahatan Digital

Meskipun beberapa pasalnya masih relevan, KUHP warisan kolonial memiliki keterbatasan yang signifikan dalam menjangkau kompleksitas kejahatan digital. KUHP dirancang dalam paradigma kejahatan fisik, sehingga banyak konsepnya yang sulit diterapkan pada dunia siber. Misalnya, KUHP tidak secara eksplisit mengatur perbuatan seperti akses ilegal ke sistem komputer (*hacking*), intersepsi data, atau serangan DDoS. Konsep "barang" dalam KUHP juga pada awalnya merujuk pada benda berwujud, sehingga memerlukan penafsiran hukum yang ekstensif untuk mencakup data dan aset digital.

Keterbatasan lainnya adalah terkait yurisdiksi. KUHP menganut asas teritorial, di mana hukum pidana Indonesia berlaku untuk kejahatan yang terjadi di wilayah Indonesia. Hal ini menjadi rumit dalam kejahatan siber yang bersifat lintas batas (*transborder*), di mana pelaku, korban, dan server bisa berada di tiga negara yang berbeda. KUHP tidak memiliki mekanisme yang memadai untuk menangani tantangan yurisdiksi dalam dunia maya ini.

Selain itu, KUHP tidak mengatur mengenai alat bukti digital. Proses pembuktian dalam KUHP dirancang untuk bukti-bukti konvensional seperti keterangan saksi, surat, dan petunjuk fisik. Keabsahan dan tata cara penyajian alat bukti elektronik tidak diatur, yang dapat menimbulkan perdebatan hukum di persidangan. Keterbatasan-keterbatasan inilah yang mendorong lahirnya undang-undang khusus (*lex specialis*) untuk mengatasi kejahatan siber.

4. Arah Pembaharuan KUHP terkait Kejahatan Siber

Menyadari keterbatasan tersebut, pembaharuan hukum pidana di Indonesia telah dilakukan melalui pengesahan Undang-Undang No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru), yang akan berlaku efektif pada tahun 2026. KUHP Baru ini secara signifikan lebih adaptif terhadap perkembangan zaman, termasuk dengan memasukkan bab khusus mengenai Tindak Pidana Teknologi Informasi. Ini merupakan langkah maju yang sangat penting, karena mengintegrasikan delik-delik siber ke dalam kodifikasi hukum pidana nasional.

Dalam KUHP Baru, perbuatan seperti mengakses sistem elektronik secara ilegal, menyadap transmisi data, mengganggu sistem elektronik, dan memproduksi atau menjual perangkat keras/lunak untuk kejahatan siber diatur secara eksplisit sebagai tindak pidana. Ini mengisi kekosongan hukum yang ada dalam KUHP lama. Dengan adanya pasal-pasal ini, penegak hukum akan memiliki dasar yang lebih kokoh untuk menindak berbagai bentuk peretasan dan kejahatan siber lainnya yang sering digunakan untuk mencuri aset kripto.

Meskipun UU ITE akan tetap berlaku sebagai *lex specialis*, kodifikasi delik siber ke dalam KUHP Baru menunjukkan pengakuan bahwa kejahatan siber bukan lagi fenomena pinggiran, melainkan bagian integral dari lanskap kriminalitas modern. Arah pembaharuan ini adalah untuk menciptakan sistem hukum pidana yang lebih komprehensif, terintegrasi, dan mampu merespons tantangan teknologi di masa depan, termasuk yang mungkin muncul dari evolusi *cryptocurrency* dan *blockchain*.

B. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang No. 11 Tahun 2008 sebagaimana telah diubah dengan UU No. 19 Tahun 2016 (dan perubahan kedua dengan UU No. 1 Tahun 2024) tentang Informasi dan Transaksi Elektronik (UU ITE) adalah payung hukum utama (*lex specialis*) untuk kejahatan siber di Indonesia. UU ini secara spesifik dirancang untuk mengatur ruang siber. Sub-bab ini akan membahas ketentuan-ketentuan pidana kunci dalam UU ITE yang relevan untuk kejahatan kripto, termasuk delik penyebaran berita bohong dan pengakuan terhadap alat bukti elektronik.

1. Ketentuan Pidana terkait Akses Ilegal, Perubahan, dan Penghilangan Informasi Elektronik

UU ITE secara tegas mengkriminalisasi perbuatan-perbuatan yang menjadi dasar dari aksi peretasan. Pasal 30 UU ITE melarang "dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun". Pasal ini dapat digunakan untuk menjerat peretas yang menyusup ke dalam server bursa kripto atau akun pengguna. Ayat-ayat selanjutnya dalam pasal ini juga melarang tindakan mengambil, mengubah, atau menghilangkan informasi elektronik, yang relevan untuk kasus pencurian data atau perusakan sistem.

Ketentuan ini sangat penting karena mengisi kekosongan dalam KUHP lama. Dengan adanya pasal ini, setiap tindakan peretasan yang bertujuan untuk mencuri aset kripto dapat dituntut, terlepas dari apakah asetnya berhasil dicuri atau tidak. Perbuatan "mengakses secara ilegal" itu sendiri sudah merupakan sebuah tindak pidana. Ini memberikan dasar hukum yang kuat bagi penegak hukum untuk menindak para peretas yang menargetkan ekosistem *cryptocurrency*.

Selain Pasal 30, Pasal 32 UU ITE juga relevan, yang melarang tindakan mengubah, merusak, atau menyembunyikan Informasi Elektronik atau Dokumen Elektronik. Pasal ini dapat diterapkan pada kasus di mana pelaku memanipulasi data transaksi atau menyembunyikan jejak digital kejahatannya. Ketentuan-ketentuan ini secara kolektif membentuk benteng pertahanan hukum terhadap berbagai bentuk serangan teknis pada infrastruktur digital.

2. Delik Penyebaran Berita Bohong yang Merugikan Konsumen

Salah satu pasal dalam UU ITE yang paling relevan untuk memberantas penipuan investasi kripto adalah Pasal 28 ayat (1). Pasal ini melarang setiap orang yang "dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik". Pasal ini sangat cocok untuk menjerat para promotor skema Ponzi, *rug pull*, atau penawaran koin fiktif yang menggunakan media sosial, situs web, atau aplikasi pesan untuk menyebarkan janji-janji palsu.

Unsur "berita bohong dan menyesatkan" terpenuhi ketika pelaku menjanjikan keuntungan pasti, teknologi revolusioner yang tidak ada, atau kemitraan fiktif. Unsur "mengakibatkan kerugian konsumen" terpenuhi ketika para investor kehilangan uang atau aset kripto mereka karena mempercayai informasi bohong tersebut. "Transaksi Elektronik" dalam konteks ini dapat diartikan secara luas untuk mencakup proses investasi atau pembelian aset kripto yang dilakukan melalui platform digital.

Pasal ini lebih spesifik daripada Pasal 378 KUHP karena secara eksplisit menyebutkan konteks "Transaksi Elektronik" dan "kerugian konsumen", membuatnya menjadi senjata hukum yang lebih tajam untuk melawan penipuan di dunia maya. Penerapan pasal ini terhadap para *influencer* atau figur publik yang mempromosikan skema investasi bodong tanpa uji tuntas (*due diligence*) juga menjadi area penegakan hukum yang penting untuk melindungi masyarakat.

3. Alat Bukti Elektronik dan Keabsahannya di Pengadilan

Salah satu kontribusi terpenting dari UU ITE adalah pengakuan formal terhadap alat bukti elektronik. Pasal 5 UU ITE menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Pasal ini kemudian merinci bahwa bukti elektronik ini merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Ini adalah terobosan fundamental yang memungkinkan kasus-kasus kejahatan siber untuk dibuktikan di pengadilan.

Berdasarkan ketentuan ini, berbagai jejak digital dapat diajukan sebagai alat bukti yang sah. Ini termasuk, namun tidak terbatas pada, log transaksi

dari *blockchain explorer*, riwayat percakapan di aplikasi pesan, data dari server bursa kripto, isi email, dan data forensik dari perangkat komputer atau ponsel pelaku. Tanpa pengakuan ini, jaksa akan sangat kesulitan untuk membuktikan kejahatan yang seluruhnya terjadi di dunia maya.

UU ITE juga menetapkan syarat formil dan materiil agar informasi dan dokumen elektronik dapat diterima sebagai bukti yang sah, yaitu harus dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan. Hal ini menuntut penegak hukum untuk memiliki kapasitas teknis dalam melakukan penyitaan dan analisis forensik digital sesuai dengan prosedur standar untuk memastikan integritas barang bukti tidak rusak dan dapat diterima oleh hakim di persidangan.

4. Studi Kasus Penerapan UU ITE pada Kejahatan Kripto

Penerapan UU ITE dalam kasus-kasus kejahatan kripto di Indonesia sudah mulai terlihat. Dalam kasus penipuan robot trading seperti Fahrenheit atau Finplan, para tersangka tidak hanya dijerat dengan Pasal 378 KUHP tentang penipuan, tetapi juga sering kali dijerat dengan Pasal 28 ayat (1) UU ITE. Jaksa menggunakan pasal ini untuk membuktikan bahwa para pelaku telah menyebarkan informasi bohong melalui media elektronik (seperti situs web dan seminar online) yang menyebabkan kerugian besar bagi para anggota sebagai konsumen.

Dalam kasus-kasus peretasan atau pencurian data, seperti kasus *phishing* atau pembobolan akun bursa, Pasal 30 dan Pasal 32 UU ITE menjadi dasar tuntutan utama. Penegak hukum akan bekerja sama dengan ahli forensik digital untuk melacak alamat IP pelaku, menganalisis *malware* yang digunakan, dan menyajikan bukti akses ilegal ke sistem korban. Putusan-putusan pengadilan yang menerima bukti-bukti digital ini dan menghukum pelaku berdasarkan UU ITE turut membentuk yurisprudensi yang penting bagi penanganan kejahatan siber di masa depan.

Meskipun demikian, penerapan UU ITE juga menghadapi tantangan, terutama dalam kasus yang melibatkan pelaku atau server di luar negeri. Proses permintaan bantuan hukum timbal balik (*Mutual Legal Assistance*) untuk mendapatkan data dari perusahaan teknologi asing sering kali memakan waktu lama dan birokratis. Namun, keberhasilan dalam beberapa

kasus menunjukkan bahwa UU ITE, dikombinasikan dengan kerja sama internasional, merupakan perangkat hukum yang vital dan semakin efektif dalam memerangi kejahatan di era digital.

C. UU Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU)

Undang-Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU) adalah instrumen hukum utama untuk memutus aliran dana hasil kejahatan. Kejahatan ekonomi digital yang menghasilkan keuntungan finansial, seperti penipuan atau peretasan kripto, hampir selalu diikuti oleh upaya pencucian uang. Sub-bab ini akan membahas ruang lingkup UU TPPU, kewajiban pelaporan bagi penyedia jasa keuangan termasuk pedagang aset kripto, dan peran sentral PPATK.

1. Definisi dan Ruang Lingkup TPPU

UU TPPU mendefinisikan pencucian uang secara luas, mencakup perbuatan menempatkan, mentransfer, membayarkan, membelanjakan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan, atau perbuatan lain atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana. Tujuannya adalah untuk menyembunyikan atau menyamarkan asal usul Harta Kekayaan tersebut. Definisi yang luas ini sangat relevan untuk menjerat berbagai modus pencucian uang menggunakan *cryptocurrency*.

Tindak pidana asal (*predicate crime*) yang hasilnya dapat menjadi objek TPPU juga sangat luas, mencakup 26 jenis kejahatan, termasuk penipuan, penggelapan, korupsi, narkotika, dan pendanaan terorisme. Ini berarti, setiap keuntungan yang diperoleh dari penipuan investasi kripto atau hasil penjualan narkotika di *dark web* yang kemudian diubah bentuknya menjadi aset kripto lain atau uang fiat, dapat dikategorikan sebagai tindak pidana pencucian uang. Pelaku dapat dijerat dengan pasal TPPU sebagai tambahan dari jeratan pidana atas kejahatan asalnya.

Keunggulan utama dari UU TPPU adalah pendekatan "ikuti jejak uang" (*follow the money*) dan kemungkinan penerapan pembuktian terbalik. Dalam beberapa kasus, terdakwa TPPU dapat diminta untuk membuktikan bahwa hartanya berasal dari sumber yang sah. Ini menjadi senjata yang sangat ampuh untuk menjerat para pelaku kejahatan ekonomi yang menyembunyikan kekayaan mereka dalam berbagai bentuk aset, termasuk *cryptocurrency*.

2. Kewajiban Pelaporan oleh Penyedia Jasa Keuangan (Termasuk Pedagang Aset Kripto)

Pilar utama dari rezim anti-pencucian uang (APU) adalah kewajiban pelaporan yang dibebankan kepada "Pihak Pelapor". Pihak Pelapor, menurut UU TPPU, mencakup penyedia jasa keuangan seperti bank, perusahaan asuransi, dan penyedia barang dan/atau jasa lain yang diatur oleh peraturan perundang-undangan. Berdasarkan Peraturan Bappebti, Pedagang Fisik Aset Kripto (PFAK) yang terdaftar secara resmi di Indonesia dikategorikan sebagai Pihak Pelapor. Ini adalah langkah krusial untuk membawa ekosistem kripto ke dalam pengawasan rezim APU.

Sebagai Pihak Pelapor, PFAK memiliki beberapa kewajiban utama. Pertama, mereka wajib menerapkan prinsip Mengenali Pengguna Jasa (*Know Your Customer* - KYC), yang meliputi verifikasi dan dokumentasi identitas pengguna. Kedua, mereka wajib melaporkan Transaksi Keuangan Mencurigakan (TKM) kepada Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). TKM dapat berupa transaksi yang tidak sesuai dengan profil pengguna, transaksi yang melibatkan dana dalam jumlah besar tanpa tujuan yang jelas, atau transaksi yang diduga terkait dengan tindak pidana.

Kewajiban ini secara efektif mengubah bursa kripto teregulasi dari yang berpotensi menjadi sarana pencucian uang menjadi garda terdepan dalam mendeteksinya. Dengan mewajibkan PFAK untuk memantau dan melaporkan aktivitas mencurigakan, regulator dapat memperoleh data intelijen keuangan yang sangat berharga untuk mengidentifikasi dan menyelidiki jaringan kejahatan. Kegagalan PFAK dalam memenuhi kewajiban ini dapat dikenai sanksi administratif yang berat, bahkan sanksi pidana.

3. Peran PPATK dalam Melacak Transaksi Mencurigakan

Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) adalah lembaga intelijen keuangan (*Financial Intelligence Unit* - FIU) Indonesia yang menjadi pusat dari rezim APU-PPT. PPATK memiliki tugas untuk menerima, menganalisis, dan meneruskan laporan transaksi keuangan mencurigakan dari Pihak Pelapor kepada lembaga penegak hukum yang berwenang, seperti Kepolisian, Kejaksaan, atau KPK. Peran PPATK menjadi semakin vital di era ekonomi digital.

Ketika sebuah PFAK melaporkan adanya transaksi kripto yang mencurigakan, PPATK akan melakukan analisis mendalam. Analisis ini tidak hanya terbatas pada data yang dilaporkan, tetapi juga dapat diperkaya dengan data dari sumber lain, termasuk analisis *on-chain* di *blockchain*. PPATK memiliki kewenangan untuk meminta informasi tambahan dari Pihak Pelapor dan, dalam kasus-kasus tertentu, dapat merekomendasikan kepada penegak hukum untuk melakukan penghentian sementara transaksi atau pemblokiran aset.

Hasil analisis PPATK yang berisi indikasi tindak pidana pencucian uang atau tindak pidana asal kemudian diserahkan kepada penegak hukum sebagai bahan awal untuk proses penyelidikan dan penyidikan. Dengan demikian, PPATK berfungsi sebagai jembatan krusial antara sektor swasta (Pihak Pelapor) dan aparat penegak hukum, mengubah data transaksi mentah menjadi intelijen keuangan yang dapat ditindaklanjuti untuk memberantas kejahatan.

4. Tantangan dalam Penerapan UU TPPU pada Aset Kripto

Meskipun kerangka hukumnya sudah ada, penerapan UU TPPU pada aset kripto menghadapi sejumlah tantangan teknis dan praktis. Tantangan pertama adalah sifat anonimitas dan pseudonimitas dari banyak aset kripto. Pelaku kejahatan dapat menggunakan *mixer*, *privacy coins*, atau teknik *chain hopping* untuk mengaburkan jejak transaksi, membuat analisis oleh PPATK dan penegak hukum menjadi sangat sulit.

Tantangan kedua adalah keberadaan bursa tidak teregulasi dan platform P2P yang beroperasi di luar jangkauan hukum Indonesia. Pelaku dapat dengan mudah memindahkan dana dari bursa teregulasi di Indonesia

ke bursa anonim di luar negeri, di mana jejaknya menjadi hilang. Kerja sama internasional untuk melacak aset di yurisdiksi yang tidak kooperatif sering kali lambat dan tidak efektif. Selain itu, kebangkitan Keuangan Terdesentralisasi (DeFi), yang tidak memiliki entitas perantara sebagai Pihak Pelapor, menciptakan tantangan regulasi yang sama sekali baru.

Tantangan ketiga adalah kapasitas teknis dari aparat penegak hukum. Investigasi TPPU yang melibatkan kripto memerlukan keahlian khusus dalam analisis forensik *blockchain* dan pemahaman mendalam tentang cara kerja ekosistem digital. Peningkatan kapasitas sumber daya manusia, investasi dalam perangkat lunak analisis, dan kerja sama erat dengan ahli dari sektor swasta menjadi kunci untuk mengatasi tantangan ini dan memastikan bahwa UU TPPU dapat ditegakkan secara efektif di dunia maya.

D. Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme (UU PP-TPPT)

Undang-Undang No. 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme (UU PP-TPPT) merupakan instrumen hukum spesifik untuk memutus urat nadi finansial kelompok teroris. Seiring dengan meningkatnya penggunaan *cryptocurrency* oleh kelompok teroris, UU ini menjadi semakin relevan. Sub-bab ini akan membahas larangan pendanaan, mekanisme pembekuan aset, dan peran kerja sama internasional dalam konteks penggunaan kripto untuk pendanaan terorisme.

1. Larangan Setiap Bentuk Pendanaan untuk Kegiatan Terorisme

UU PP-TPPT secara sangat luas melarang setiap perbuatan dalam rangka menyediakan, mengumpulkan, memberikan, atau meminjamkan dana, baik langsung maupun tidak langsung, dengan maksud untuk digunakan dan/atau yang diketahui akan digunakan untuk melakukan kegiatan terorisme. Frasa "dana" dalam UU ini diartikan secara luas mencakup segala bentuk aset, baik berwujud maupun tidak berwujud, bergerak maupun tidak bergerak, termasuk aset kripto. Dengan demikian, memberikan donasi kepada kelompok teroris dalam bentuk Bitcoin, Monero, atau aset kripto lainnya secara jelas merupakan tindak pidana berdasarkan UU ini.

Larangan ini berlaku terlepas dari jumlah dana yang diberikan. Bahkan donasi dalam jumlah kecil (pendanaan mikro) yang dikirim melalui *cryptocurrency* sudah dapat memenuhi unsur tindak pidana. UU ini juga mengadopsi prinsip "kesengajaan atau pengetahuan", artinya seseorang dapat dipidana jika ia sengaja mendanai terorisme atau setidaknya patut menduga bahwa dana yang ia berikan akan digunakan untuk tujuan tersebut. Hal ini penting untuk menjerat para simpatisan yang mungkin berdalih tidak mengetahui secara pasti penggunaan akhir dari donasi mereka.

Dengan cakupan yang luas ini, UU PP-TPPT memberikan dasar hukum yang sangat kuat bagi Densus 88 Antiteror dan lembaga terkait lainnya untuk menindak siapa saja yang terlibat dalam rantai pasokan pendanaan terorisme, termasuk mereka yang hanya berperan sebagai fasilitator transfer dana menggunakan *cryptocurrency*.

2. Mekanisme Pembekuan Aset Terduga Teroris

Salah satu fitur paling kuat dari UU PP-TPPT adalah mekanisme pembekuan aset yang cepat. Berdasarkan laporan dari penegak hukum atau informasi dari daftar terduga teroris yang dikeluarkan oleh PBB, PPATK dapat memerintahkan Pihak Pelapor (termasuk PFAK) untuk segera membekukan seluruh dana atau aset yang dimiliki atau dikuasai oleh individu atau korporasi yang masuk dalam daftar tersebut. Proses ini dapat dilakukan secara cepat tanpa memerlukan putusan pengadilan terlebih dahulu, untuk mencegah aset tersebut dipindahkan atau digunakan lebih lanjut.

Dalam konteks *cryptocurrency*, mekanisme ini sangat vital. Jika seorang terduga teroris teridentifikasi memiliki akun di sebuah bursa kripto yang terdaftar di Indonesia, PPATK dapat langsung memerintahkan bursa tersebut untuk membekukan semua aset kripto di akun tersebut. Bursa kemudian wajib untuk segera mematuhi perintah tersebut. Mekanisme ini merupakan implementasi dari prinsip *sadd al-żarī'ah* (menutup jalan keburukan) dalam hukum positif, yaitu dengan melumpuhkan kapasitas finansial teroris secepat mungkin.

Tantangan terbesar dalam implementasinya adalah jika terduga teroris menyimpan asetnya di dompet pribadi (*non-custodial wallet*) atau di bursa luar negeri yang tidak kooperatif. Dalam kasus dompet pribadi, tidak ada pihak ketiga yang dapat diperintahkan untuk melakukan pembekuan; aset hanya dapat disita jika penegak hukum berhasil mendapatkan akses fisik atau digital ke *private key* pelaku. Hal ini menunjukkan batasan dari mekanisme pembekuan aset terpusat dalam menghadapi ekosistem yang terdesentralisasi.

3. Kerjasama Internasional dalam Memutus Jaringan Pendanaan

Mengingat sifat pendanaan terorisme yang global dan penggunaan *cryptocurrency* yang lintas batas, kerja sama internasional menjadi kunci yang tidak terpisahkan dari upaya pemberantasan. UU PP-TPPT memberikan landasan hukum bagi Indonesia untuk menjalin kerja sama dengan negara lain dan organisasi internasional. Kerja sama ini dapat berbentuk pertukaran informasi intelijen keuangan, bantuan hukum timbal balik (*Mutual Legal Assistance* - MLA), hingga ekstradisi pelaku.

PPATK, sebagai anggota dari Egmont Group (jaringan global unit intelijen keuangan), dapat bertukar informasi mengenai transaksi kripto yang mencurigakan dengan FIU dari negara lain. Misalnya, jika PPATK mendeteksi aliran dana dari sebuah bursa di Indonesia ke alamat yang terkait dengan terorisme di negara lain, informasi tersebut dapat segera dibagikan kepada otoritas di negara tujuan untuk ditindaklanjuti. Sebaliknya, Indonesia juga dapat menerima informasi dari negara lain mengenai warganya yang terlibat dalam pendanaan terorisme menggunakan platform domestik.

Kerja sama ini juga penting dalam proses pembekuan dan perampasan aset. Jika aset hasil pendanaan terorisme yang berasal dari Indonesia terdeteksi berada di negara lain, pemerintah Indonesia dapat mengajukan permintaan MLA kepada negara tersebut untuk membekukan dan akhirnya menyita aset tersebut. Meskipun prosesnya sering kali kompleks dan memakan waktu, kerja sama internasional adalah satu-satunya cara untuk mengejar jaringan pendanaan teroris yang beroperasi secara global di dunia maya.

4. Implementasi UU PP-TPPT dalam Kasus Kripto

Implementasi UU PP-TPPT dalam kasus-kasus yang melibatkan *cryptocurrency* di Indonesia sudah mulai berjalan, meskipun tantangannya besar. Pengungkapan oleh Densus 88 mengenai adanya terduga teroris yang menggunakan Bitcoin untuk mengirim dana ke Suriah menjadi studi kasus awal yang penting. Dalam kasus tersebut, penyidik berhasil melacak transaksi dari pembelian Bitcoin di bursa domestik hingga pengirimannya ke luar negeri. Pelaku dapat dijerat dengan UU PP-TPPT karena perbuatannya secara jelas memenuhi unsur "menyediakan dana" untuk kegiatan terorisme.

Kasus ini dan kasus-kasus serupa lainnya mendorong peningkatan kolaborasi antara Densus 88, PPATK, dan PFAK yang terdaftar. PFAK kini menjadi salah satu sumber informasi penting bagi penegak hukum dalam mendeteksi aktivitas pendanaan terorisme. Pelatihan dan peningkatan kapasitas bagi para analis di PPATK dan penyidik di Densus 88 mengenai teknik-teknik analisis *blockchain* terus dilakukan untuk mengimbangi modus operandi pelaku yang semakin canggih.

Ke depan, tantangan utama adalah mengawasi titik-titik rawan yang sulit dijangkau, seperti transaksi P2P informal, penggunaan *mixer*, dan platform DeFi. Namun, keberhasilan awal dalam menerapkan UU PP-TPPT pada kasus kripto menunjukkan bahwa kerangka hukum yang ada, jika didukung dengan kapasitas teknis dan kerja sama yang kuat, memiliki potensi untuk tetap efektif dalam memitigasi ancaman pendanaan terorisme di era digital.

E. Regulasi Sektoral: Peraturan BAPPEBTI

Selain undang-undang pidana umum dan khusus, terdapat regulasi sektoral yang secara spesifik mengatur ekosistem aset kripto di Indonesia. Peraturan yang dikeluarkan oleh Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) ini menjadi kerangka hukum administratif yang mengatur perdagangan aset kripto sebagai komoditas. Sub-bab ini akan mengkaji kedudukan hukum aset kripto, kewajiban yang dibebankan pada Pedagang Fisik Aset Kripto (PFAK), serta mekanisme APU-PPT dan sanksi dalam ranah regulasi Bappebti.

1. Kedudukan Hukum Aset Kripto sebagai Komoditas

Langkah paling fundamental yang diambil oleh Bappebti adalah memberikan status hukum yang jelas bagi aset kripto di Indonesia. Melalui Peraturan Bappebti No. 5 Tahun 2019 (dan peraturan-peraturan pembaruannya), Bappebti menetapkan bahwa Aset Kripto adalah "komoditi tidak berwujud yang berbentuk digital" yang dapat menjadi subjek Kontrak Berjangka, Opsi, dan/atau turunan lainnya. Dengan definisi ini, Bappebti secara resmi melegalkan perdagangan aset kripto, bukan sebagai mata uang, melainkan sebagai komoditas investasi.

Penetapan ini memiliki implikasi hukum yang sangat penting. Pertama, ia memberikan kepastian hukum bagi para investor dan pelaku usaha di industri kripto Indonesia. Kedua, ia membawa aktivitas perdagangan kripto dari yang semula tidak diatur (*unregulated*) ke dalam ranah yang diawasi (*regulated*), sehingga memungkinkan pemerintah untuk memberlakukan aturan main. Ketiga, Bappebti juga merilis daftar aset kripto yang legal untuk diperdagangkan di Indonesia, yang berfungsi sebagai filter awal untuk melindungi masyarakat dari koin-koin fiktif atau berbahaya.

Keputusan untuk mengkategorikan kripto sebagai komoditas menempatkannya di bawah yurisdiksi Bappebti, bukan Otoritas Jasa Keuangan (OJK) yang mengawasi pasar modal atau Bank Indonesia yang mengawasi sistem pembayaran. Meskipun demikian, seiring dengan perkembangan industri, koordinasi antar lembaga ini menjadi semakin krusial untuk mencegah adanya celah regulasi.

2. Kewajiban Pedagang Fisik Aset Kripto (PFAK)

Untuk dapat beroperasi secara legal di Indonesia, platform bursa kripto harus terdaftar di Bappebti sebagai Calon Pedagang Fisik Aset Kripto (CPFAK) dan pada akhirnya menjadi Pedagang Fisik Aset Kripto (PFAK). Peraturan Bappebti menetapkan serangkaian kewajiban ketat yang harus dipenuhi oleh PFAK. Kewajiban ini mencakup persyaratan modal minimum, sistem keamanan teknologi informasi yang andal, tata kelola perusahaan yang baik, dan kewajiban untuk menyimpan sebagian besar aset nasabah di *cold wallet* untuk mencegah peretasan.

Selain itu, PFAK diwajibkan untuk memiliki mekanisme penyelesaian sengketa bagi nasabah dan harus transparan mengenai risiko investasi

aset kripto. Mereka juga harus bekerja sama dengan lembaga kliring berjangka untuk menjamin penyelesaian transaksi dan lembaga depositori untuk penyimpanan aset. Seluruh rangkaian kewajiban ini bertujuan untuk menciptakan lingkungan perdagangan yang lebih aman, adil, dan terpercaya bagi masyarakat.

Dengan adanya persyaratan ini, Bappebti secara efektif menciptakan standar industri. Hanya perusahaan yang memiliki modal, teknologi, dan komitmen terhadap keamanan dan kepatuhan yang dapat beroperasi. Ini membantu menyaring pelaku usaha yang tidak serius atau berpotensi merugikan konsumen, meskipun pengawasan terhadap implementasi kewajiban ini di lapangan tetap menjadi tantangan.

3. Mekanisme Anti-Pencucian Uang (APU) dan Pencegahan Pendanaan Terorisme (PPT) di PFAK

Salah satu kewajiban terpenting yang dibebankan oleh Bappebti kepada PFAK adalah penerapan program Anti-Pencucian Uang (APU) dan Pencegahan Pendanaan Terorisme (PPT), yang sejalan dengan UU TPPU dan UU PP-TPPT. Peraturan Bappebti secara eksplisit mewajibkan PFAK untuk menerapkan Prinsip Mengenali Pengguna Jasa (PMPJ) atau KYC. Ini berarti PFAK harus melakukan identifikasi, verifikasi, dan pemantauan terhadap semua penggunanya.

Proses KYC biasanya melibatkan pengumpulan data identitas seperti KTP, swafoto dengan KTP, dan verifikasi biometrik. Data ini penting untuk memastikan bahwa akun tidak dibuka secara anonim. Selanjutnya, PFAK wajib untuk memantau transaksi nasabah dan melaporkan Transaksi Keuangan Mencurigakan (TKM) kepada PPATK. Bappebti bekerja sama dengan PPATK dalam menyusun pedoman mengenai indikator TKM di sektor aset kripto, misalnya transaksi dalam jumlah besar yang tidak wajar, transaksi yang terpecah-pecah untuk menghindari ambang batas pelaporan (*structuring*), atau transaksi yang melibatkan alamat dompet yang diketahui terkait dengan kejahatan.

Dengan menjadikan PFAK sebagai "gerbang" yang diawasi, regulasi Bappebti secara signifikan mengurangi risiko penggunaan bursa domestik untuk tujuan pencucian uang dan pendanaan terorisme. Regulasi ini menyelaraskan industri aset kripto Indonesia dengan standar

internasional yang ditetapkan oleh Financial Action Task Force (FATF), yang merekomendasikan agar semua penyedia layanan aset virtual (VASP) tunduk pada kewajiban APU-PPT.

4. Sanksi Administratif dan Pidana bagi Pelanggar Regulasi

Untuk memastikan kepatuhan, Peraturan Bappebti dilengkapi dengan mekanisme sanksi yang jelas. Pelanggaran terhadap kewajiban yang ditetapkan dapat dikenai sanksi administratif. Sanksi ini bersifat bertingkat, mulai dari peringatan tertulis, denda, pembekuan kegiatan usaha, hingga yang paling berat adalah pencabutan izin sebagai PFAK. Sanksi administratif ini memberikan Bappebti alat untuk menegakkan disiplin industri dan memastikan bahwa PFAK beroperasi sesuai dengan aturan yang berlaku.

Misalnya, jika sebuah PFAK terbukti lalai dalam menerapkan program APU-PPT, seperti tidak melakukan KYC dengan benar atau gagal melaporkan TKM, Bappebti dapat menjatuhkan sanksi. Sanksi ini tidak hanya bersifat menghukum, tetapi juga sebagai insentif bagi PFAK lain untuk meningkatkan sistem kepatuhan mereka. Pengawasan dan audit secara berkala oleh Bappebti menjadi kunci untuk memastikan efektivitas dari penegakan sanksi administratif ini.

Selain sanksi administratif dari Bappebti, para direksi atau pejabat PFAK yang secara sengaja melanggar ketentuan pidana dalam UU TPPU atau UU PP-TPPT juga dapat dimintai pertanggungjawaban secara personal. Misalnya, jika seorang pejabat bursa terbukti secara aktif membantu nasabah untuk melakukan pencucian uang, ia dapat dituntut secara pidana berdasarkan UU TPPU. Kombinasi antara sanksi administratif dari regulator sektoral dan ancaman sanksi pidana dari undang-undang umum menciptakan kerangka penegakan hukum yang berlapis dan komprehensif.

Analisis Mendalam Konsep Kunci Bab 6: Kerangka Hukum Positif Berlapis

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk menunjukkan bahwa tidak ada satu pun "undang-undang kripto" yang tunggal di Indonesia. Sebaliknya, penegakan

hukum harus menggunakan pendekatan multi-instrumen, dengan mengombinasikan berbagai undang-undang yang ada. Tujuannya adalah untuk:

1. Memetakan Arsenal Hukum: Mengidentifikasi dan memetakan semua "senjata" (undang-undang) yang tersedia bagi aparat penegak hukum.
2. Menganalisis Fungsi Spesifik: Menjelaskan peran dan fungsi spesifik dari setiap undang-undang dalam menjerat aspek-aspek yang berbeda dari kejahatan kripto.
3. Mengidentifikasi Kekuatan dan Kelemahan: Menyoroti pasal-pasal mana yang efektif dan di mana letak keterbatasan atau "lubang" dalam setiap lapisan hukum.
4. Menunjukkan Sinergi dan Tumpang Tindih: Menggambarkan bagaimana undang-undang ini saling melengkapi (sinergi) dan terkadang berpotensi menimbulkan konflik norma atau tumpang tindih kewenangan.

Ini adalah pandangan dari "ruang mesin" penegakan hukum di Indonesia, melihat bagaimana berbagai komponen hukum bekerja bersama.

Elemen-Elemen Kunci dalam Kerangka Berlapis:

1. Lapisan Hukum Pidana Umum (Dasar): Fondasi hukum pidana yang berlaku untuk semua jenis kejahatan.
2. Lapisan Hukum Pidana Khusus (Spesifik): Undang-undang yang dirancang untuk mengatasi jenis kejahatan tertentu yang kompleks dan modern.
3. Lapisan Hukum Administratif (Regulasi Sektoral): Peraturan yang mengatur industrinya secara spesifik, dengan fokus pada pencegahan dan pengawasan, bukan pemidanaan.

Analisis Komparatif: Lapisan-Lapisan Kerangka Hukum Indonesia

Tabel berikut membedah fungsi dan peran dari setiap lapisan hukum dalam menanggulangi kejahatan *cryptocurrency*.

Lapisan Hukum	KUHP (Kitab Undang-Undang Hukum Pidana)	UU ITE (Informasi & Transaksi Elektronik)	UU TPPU & UU PP-TPPT	Peraturan BAPPEBTI
Fungsi Utama	Lapisan Dasar. Menjerat esensi perbuatan kejahatan konvensional (penipuan, penggelapan).	Lapisan Siber. Menjerat metode/medium digital yang digunakan dalam kejahatan.	Lapisan Keuangan. Menjerat aliran dana hasil kejahatan dan pendanaan terorisme.	**Lapisan Industri**. Mengatur **pelaku usaha** di sektor aset kripto untuk pencegahan.
Fokus Delik	Kejahatan terhadap harta benda dan kepercayaan.	Kejahatan yang berkaitan dengan informasi, dokumen, dan sistem elektronik.	Kejahatan menyembunyikan/ menyamarkan harta hasil pidana dan mendanai teror.	Pelanggaran administratif terkait perizinan, kepatuhan, dan perlindungan konsumen.
Contoh Pasal Kunci	Pasal 378 (Penipuan), Pasal 372 (Penggelapan).	Pasal 28 (Berita Bohong), Pasal 30 (Akses Ilegal/Hacking), Pasal 32 (Merusak Sistem).	Pasal 3, 4, 5 UU TPPU (Pencucian Uang), Pasal 4 UU PP-TPPT (Pendanaan Terorisme).	Kewajiban KYC, pelaporan, keamanan sistem, modal disetor.
Kekuatan Utama	Fleksibel & Teruji. Konsep penipuan dan penggelapan sudah mapan dalam yurisprudensi.	Sangat Spesifik. Secara eksplisit mengkriminalisasi peretasan dan penyebaran berita bohong online. Mengakui alat bukti digital.	Sangat Kuat. Memungkinkan perampasan aset dan mengikuti aliran dana (*follow the money*). Beban pembuktian terbalik.	Preventif. Mencegah kejahatan terjadi dengan mewajibkan standar kepatuhan pada pelaku industri.

Lapisan Hukum	KUHP (Kitab Undang-Undang Hukum Pidana)	UU ITE (Informasi & Transaksi Elektronik)	UU TPPU & UU PP-TPPT	Peraturan BAPPEBTI
Kelemahan/ Tantangan	Kuno & Tidak Spesifik. Tidak dirancang untuk era digital. Konsep "barang" bisa diperdebatkan.	"Pasal Karet". Pasal 28 sering dianggap multitafsir. Pembuktian niat jahat bisa sulit.	Membutuhkan Kejahatan Asal (*Predicate Crime*). TPPU tidak bisa berdiri sendiri tanpa adanya tindak pidana awal.	Sanksi Dominan Administratif. Tidak bisa langsung memidanakan, fokus pada denda atau pencabutan izin. Kewenangan terbatas pada pedagang terdaftar.
Penerapan pada Kasus Kripto	Menjerat pelaku investasi bodong (robot trading) karena unsur tipu muslihatnya.	Menjerat *influencer* yang mempromosikan investasi bodong, dan *hacker* yang meretas bursa.	Menjerat siapa pun yang menerima dan menikmati hasil kejahatan kripto, serta yang mengirim dana untuk terorisme.	Memberikan sanksi kepada bursa kripto yang lalai dalam menerapkan KYC atau gagal melaporkan transaksi mencurigakan.

Kontribusi Konsep Kerangka Berlapis dalam Bab 6:

Konsep ini adalah peta jalan penegakan hukum positif di Indonesia.

1. Menunjukkan Kompleksitas Penindakan: Bab 6 menjelaskan bahwa menindak kejahatan kripto bukanlah pekerjaan satu undang-undang, melainkan sebuah operasi gabungan yang membutuhkan pemahaman mendalam tentang berbagai instrumen hukum. Jaksa sering kali menggunakan dakwaan berlapis dari berbagai UU ini.
2. Menjadi Dasar untuk Bab Analisis Kasus (Bab 8): Analisis studi kasus di Bab 8 akan secara langsung merujuk pada kerangka ini. Pembahasan kasus Fahrenheit atau Doni Salmanan akan membedah bagaimana Jaksa menggunakan kombinasi pasal dari KUHP, UU ITE, dan UU TPPU.
3. Mengidentifikasi Celah Regulasi: Dengan memetakan apa yang sudah dicakup oleh setiap UU, bab ini secara implisit menyoroti apa yang belum tercakup. Hal ini mengarah pada kesimpulan tentang perlunya sebuah undang-undang khusus tentang aset digital yang lebih komprehensif, sebuah rekomendasi yang akan diperkuat di bab-bab akhir.

Secara ringkas, Bab 6 menyajikan "kotak peralatan" hukum yang dimiliki Indonesia. Ia membongkar setiap "alat" (undang-undang), menjelaskan fungsinya, kekuatan, dan kelemahannya. Pemahaman ini sangat penting untuk menilai apakah perangkat hukum yang ada saat ini sudah memadai, atau apakah Indonesia memerlukan "alat" baru yang dirancang khusus untuk menghadapi tantangan unik dari ekonomi digital.

BAB 7

Sinkronisasi dan Harmonisasi Hukum Pidana Islam dan Hukum Positif

Setelah menjelajahi secara terpisah ranah hukum pidana Islam (Bab 5) dan hukum positif Indonesia (Bab 6), bab terakhir ini tiba pada sebuah jembatan konseptual: sinkronisasi dan harmonisasi. Dalam konteks masyarakat Indonesia yang mayoritas Muslim dan sekaligus terikat pada sistem hukum nasional, pertanyaan tentang bagaimana kedua sistem hukum ini dapat berjalan beriringan menjadi sangat krusial. Bab ini tidak bertujuan untuk menggabungkan kedua sistem secara formal, melainkan untuk mengidentifikasi titik-titik temu, keselarasan prinsip, dan potensi saling melengkapi dalam menghadapi musuh bersama, yaitu kejahatan ekonomi digital. *Research gap* yang hendak diisi adalah kurangnya analisis yang secara jernih memetakan area konvergensi dan divergensi antara hukum pidana Islam dan hukum positif Indonesia dalam konteks kejahatan siber, serta mengeksplorasi bagaimana nilai-nilai dari satu sistem dapat memperkaya sistem lainnya. Pertanyaan penelitian utama yang akan dijawab adalah: Di titik mana saja terjadi keselarasan filosofis dan praktis antara hukum pidana Islam dan hukum positif Indonesia dalam memberantas kejahatan *cryptocurrency*, dan bagaimana potensi sinergi ini dapat dioptimalkan untuk pembaharuan hukum di masa depan?

A. Titik Temu Filosofis: Perlindungan Kepentingan Publik

Meskipun hukum pidana Islam bersumber dari wahyu dan hukum positif bersumber dari kedaulatan negara, keduanya bertemu pada tujuan fundamental yang sama: melindungi kepentingan publik dan mewujudkan kemaslahatan. Sub-bab ini akan mengeksplorasi titik-titik temu filosofis tersebut, dengan membandingkan konsep *Maqāshid al-Sharī'ah* dengan tujuan hukum nasional. Fokus akan diberikan pada prinsip perlindungan harta, penjagaan keamanan, dan nilai keadilan sebagai fondasi bersama yang melandasi upaya pemberantasan kejahatan.

1. Maqashid al-Shari'ah dan Tujuan Hukum Nasional

Titik temu paling fundamental terletak pada tujuan luhur di balik legislasi. Hukum Islam didasarkan pada *Maqāshid al-Sharī'ah*, yaitu tujuan-tujuan syariah untuk mewujudkan kemaslahatan (*maṣlaḥah*) bagi umat manusia. Kelima tujuan pokoknya (*al-ḍarūriyyāt al-khamsah*) adalah perlindungan terhadap agama, jiwa, akal, keturunan, dan harta. Di sisi lain,

tujuan hukum nasional Indonesia, sebagaimana tersirat dalam Pembukaan UUD 1945, adalah untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia.

Jika dianalisis lebih dalam, terdapat korelasi yang kuat antara kedua tujuan ini. "Melindungi segenap bangsa" beririsan langsung dengan perlindungan jiwa (*ḥifẓ al-nafs*). "Memajukan kesejahteraan umum" sangat selaras dengan perlindungan harta (*ḥifẓ al-māl*) dan pemenuhan kebutuhan ekonomi masyarakat. "Mencerdaskan kehidupan bangsa" sejalan dengan perlindungan akal (*ḥifẓ al-'aql*). Dan "melaksanakan ketertiban" adalah cerminan dari tujuan syariah secara umum untuk menolak kerusakan (*dar' al-mafāsid*) dan menjaga keamanan (*ḥifẓ al-amn*). Konvergensi pada level teleologis (tujuan) ini menjadi dasar bagi kemungkinan harmonisasi pada level implementasi.

Pemberantasan kejahatan ekonomi digital, dari kedua perspektif, bukanlah tujuan itu sendiri, melainkan sarana untuk mencapai tujuan yang lebih tinggi. Dari perspektif Islam, ia adalah sarana untuk melindungi harta umat dan mencegah kerusakan. Dari perspektif hukum nasional, ia adalah sarana untuk melindungi warga negara dari kerugian, menjaga stabilitas ekonomi, dan memelihara ketertiban umum. Kesamaan tujuan fundamental inilah yang membuat kedua sistem hukum dapat bergerak ke arah yang sama dalam menghadapi ancaman kejahatan *cryptocurrency*.

2. Perlindungan Harta (Hifzh al-Maal) dan Perlindungan Properti

Salah satu area konvergensi yang paling jelas adalah pada prinsip perlindungan harta. *Ḥifẓ al-māl* adalah salah satu dari lima pilar *Maqāshid al-Sharī'ah*, yang menunjukkan betapa pentingnya perlindungan terhadap hak milik yang sah dalam Islam. Syariah menetapkan aturan yang ketat untuk melarang pencurian, penipuan, penggelapan, dan segala bentuk perolehan harta secara batil. Sanksi-sanksi pidana dalam Islam, baik *hudūd* maupun *ta'zīr*, berfungsi sebagai benteng untuk melindungi pilar ini.

Di sisi lain, hukum positif Indonesia, yang berakar pada tradisi hukum sipil, juga menempatkan perlindungan hak milik (Pasal 570 KUHPerdata lama) sebagai salah satu prinsip utamanya. Seluruh bangunan hukum pidana yang berkaitan dengan kejahatan terhadap kekayaan, seperti Pasal

378 KUHP (penipuan) dan Pasal 362 KUHP (pencurian), pada dasarnya bertujuan untuk melindungi hak properti warga negara. Upaya negara untuk memberantas penipuan investasi kripto dan peretasan dompet digital adalah manifestasi modern dari fungsi perlindungan properti ini.

Dengan demikian, ketika negara melalui aparat penegak hukumnya menindak para pelaku penipuan atau pencurian aset kripto, tindakan tersebut secara substansial selaras dengan prinsip *ḥifẓ al-māl*. Baik hukum Islam maupun hukum positif sama-sama memandang bahwa perampasan harta orang lain secara tidak sah, baik dalam bentuk fisik maupun digital, adalah sebuah kejahatan yang harus ditindak. Kesamaan pandangan terhadap objek yang dilindungi ini mempermudah proses sinkronisasi dalam penegakan hukumnya.

3. Menjaga Keamanan (Hifzh al-Nafs, Hifzh al-Amn) dan Ketertiban Umum

Titik temu filosofis lainnya adalah pada kewajiban negara untuk menjaga keamanan dan ketertiban. Dalam hukum Islam, perlindungan terhadap jiwa (*ḥifẓ al-nafs*) dan keamanan publik (*ḥifẓ al-amn*) adalah prioritas utama. Kejahatan-kejahatan serius seperti *ḥirābah* (terorisme/perampokan) dan *bughāt* (pemberontakan) diancam dengan sanksi yang sangat berat karena dampaknya yang merusak tatanan sosial dan mengancam nyawa manusia. Negara memiliki mandat penuh untuk menggunakan kekuatan demi memberantas ancaman-ancaman tersebut.

Paralel dengan ini, tujuan utama negara dalam hukum positif adalah menjaga ketertiban umum dan keamanan nasional. Pemberantasan tindak pidana pendanaan terorisme dan kejahatan terorganisir lainnya adalah perwujudan dari fungsi fundamental negara ini. Ketika negara menggunakan UU PP-TPPT untuk memblokir aliran dana kripto ke kelompok teroris, atau menggunakan UU TPPU untuk membongkar sindikat pencucian uang, tindakan tersebut sepenuhnya sejalan dengan semangat hukum Islam untuk memerangi kejahatan yang mengancam keamanan kolektif.

Dalam konteks ini, baik hukum Islam maupun hukum positif memandang kejahatan seperti pendanaan terorisme bukan lagi sebagai kejahatan biasa, melainkan sebagai kejahatan luar biasa (*extraordinary crime*). Keduanya

memberikan legitimasi kepada negara untuk mengambil langkah-langkah tegas dan preventif, seperti pembekuan aset tanpa proses pengadilan awal, demi mencegah terjadinya bahaya yang lebih besar. Kesamaan dalam memandang tingkat ancaman ini memungkinkan adanya sinergi dalam strategi penanggulangan.

4. Nilai Keadilan sebagai Fondasi Bersama

Di atas semua prinsip teknis, nilai keadilan (*al-'adl*) menjadi fondasi bersama yang paling luhur bagi kedua sistem hukum. Hukum Islam menempatkan keadilan sebagai salah satu nilai tertingginya, yang harus ditegakkan dalam setiap aspek kehidupan, termasuk dalam proses peradilan pidana. Keadilan dalam Islam mencakup keadilan retributif (hukuman yang setimpal), keadilan distributif (pembagian hak yang adil), dan keadilan restoratif (pemulihan hubungan dan kerugian). Menghukum pelaku, mengembalikan harta curian kepada korban, dan mencegah kejahatan di masa depan adalah bagian dari penegakan keadilan.

Demikian pula, sistem hukum nasional Indonesia berasaskan pada Pancasila, di mana sila kedua "Kemanusiaan yang adil dan beradab" dan sila kelima "Keadilan sosial bagi seluruh rakyat Indonesia" menjadi landasan moralnya. Proses peradilan pidana di Indonesia, mulai dari penyelidikan hingga putusan hakim, idealnya bertujuan untuk mencapai keadilan materiil, bukan sekadar keadilan formal. Hakim diharapkan untuk menggali nilai-nilai hukum dan rasa keadilan yang hidup dalam masyarakat.

Ketika seorang hakim di pengadilan negeri menjatuhkan hukuman penjara yang berat bagi seorang penipu investasi kripto dan sekaligus memerintahkan perampasan asetnya untuk dikembalikan kepada para korban, putusan tersebut adalah manifestasi dari nilai keadilan yang diakui oleh kedua sistem hukum. Upaya untuk menghukum yang bersalah dan memulihkan hak yang terzalimi adalah titik temu universal yang menjembatani perbedaan sumber dan prosedur antara hukum pidana Islam dan hukum positif.

B. Konsep Ta'zir dan Kewenangan Legislasi Negara

Apabila titik temu filosofis menjadi fondasi, maka konsep *ta'zīr* adalah jembatan praktis yang paling vital dalam menghubungkan hukum pidana Islam dengan hukum positif modern. Sub-bab ini akan berargumen bahwa kewenangan negara untuk membuat undang-undang pidana dapat dipandang sebagai manifestasi dari kewenangan menetapkan *jarīmah ta'zīr*. Akan dianalisis bagaimana UU ITE dan UU TPPU dapat dilihat dalam kerangka ini, serta kesesuaian sanksinya dengan prinsip-prinsip hukuman *ta'zīr*.

1. Ta'zir sebagai Ruang bagi Negara untuk Membuat Regulasi Pidana

Seperti yang telah dibahas pada Bab 2, *jarīmah ta'zīr* adalah kategori tindak pidana yang jenis perbuatan dan sanksinya tidak ditetapkan secara spesifik oleh Al-Qur'an atau Sunnah. Penentuannya diserahkan sepenuhnya kepada kebijakan penguasa (*ulil amri*) demi mewujudkan kemaslahatan umum. Konsep ini memberikan ruang fleksibilitas yang sangat luas bagi hukum Islam untuk beradaptasi dengan perkembangan zaman dan munculnya bentuk-bentuk kejahatan baru yang tidak dikenal pada masa klasik.

Dalam konteks negara-bangsa modern seperti Indonesia, kewenangan *ulil amri* ini terwujud dalam fungsi legislasi yang dimiliki oleh negara (Pemerintah bersama DPR). Ketika negara membuat dan mengesahkan sebuah undang-undang pidana untuk merespons suatu masalah sosial, dari perspektif *siyāsah syar'iyyah* (fikih ketatanegaraan), tindakan tersebut dapat dipandang sebagai proses penetapan *jarīmah ta'zīr*. Undang-undang tersebut menjadi "nash" modern yang mengikat bagi seluruh warga negara.

Dengan demikian, konsep *ta'zīr* memberikan legitimasi fikih bagi keberadaan hukum pidana positif yang dibuat oleh negara. Selama undang-undang tersebut tidak bertentangan dengan prinsip-prinsip syariah yang lebih tinggi (misalnya, dengan menghalalkan yang haram secara qath'i), maka ia sah dan menjadi bagian dari sistem hukum yang harus ditaati oleh umat Islam. Ini adalah mekanisme kunci yang memungkinkan hukum Islam untuk tetap relevan dalam struktur negara modern.

2. UU ITE dan UU TPPU sebagai Bentuk Konkret dari Jarimah Ta'zir

Berdasarkan kerangka pemikiran di atas, undang-undang yang secara spesifik dibuat untuk menanggulangi kejahatan ekonomi digital dapat dilihat sebagai bentuk konkret dari legislasi *ta'zīr*. Kejahatan seperti peretasan, penyebaran berita bohong untuk penipuan, dan pencucian uang adalah perbuatan-perbuatan yang tidak diatur secara spesifik dalam kategori *hudūd* atau *qiṣāṣ*. Oleh karena itu, negara memiliki wewenang dan kewajiban untuk mengkriminalisasikannya demi melindungi masyarakat dari *mafsadah* (kerusakan) yang ditimbulkannya.

Undang-Undang ITE, yang mengkriminalisasi akses ilegal (Pasal 30) dan penyebaran berita bohong yang merugikan konsumen (Pasal 28), adalah contoh sempurna dari penetapan *jarīmah ta'zīr* untuk melindungi harta dan ketertiban di ruang siber. Demikian pula, UU TPPU, yang mengkriminalisasi upaya menyembunyikan hasil kejahatan, adalah bentuk *ta'zīr* untuk mencegah perbuatan "tolong-menolong dalam dosa" (*i'ānah 'alā al-ma'ṣiyah*) dan untuk memotong urat nadi finansial kejahatan terorganisir.

Dengan memandang undang-undang ini sebagai bentuk *ta'zīr*, maka penegakan hukum yang dilakukan oleh aparat negara berdasarkan undang-undang tersebut juga memperoleh legitimasi dari perspektif hukum Islam. Seorang polisi yang menyelidiki kasus penipuan kripto berdasarkan UU ITE, seorang jaksa yang menuntutnya, dan seorang hakim yang menghukumnya, semuanya dapat dipandang sedang menjalankan fungsi penegakan *jarīmah ta'zīr* yang telah ditetapkan oleh *ulil amri* yang sah.

3. Kesesuaian Sanksi dalam Hukum Positif dengan Prinsip Ta'zir

Prinsip utama dari hukuman *ta'zīr* adalah fleksibilitas dan proporsionalitas. Hakim memiliki diskresi untuk memilih jenis dan kadar hukuman yang paling sesuai dengan kejahatan dan pelakunya, mulai dari teguran, denda, penjara, hingga hukuman yang lebih berat. Jika kita melihat sanksi-sanksi yang diatur dalam hukum positif Indonesia untuk kejahatan siber, kita akan menemukan kesesuaian yang tinggi dengan prinsip ini.

UU ITE dan UU TPPU, misalnya, menetapkan sanksi pidana dalam bentuk penjara dan denda dengan rentang minimum dan maksimum. Adanya rentang ini memberikan ruang bagi hakim untuk menggunakan

diskresinya, mempertimbangkan faktor-faktor yang memberatkan dan meringankan, sama seperti dalam penjatuhan hukuman *ta'zīr*. Sanksi penjara (*al-ḥabs*) dan denda (*al-gharāmah*) adalah dua bentuk hukuman *ta'zīr* yang paling umum diakui dalam literatur fikih.

Selain itu, hukum positif juga mengenal sanksi tambahan, seperti pencabutan hak-hak tertentu atau pengumuman putusan hakim, yang paralel dengan konsep hukuman *tashhīr* (mempublikasikan pelaku) dalam fikih. Mekanisme perampasan aset dalam UU TPPU juga sangat sejalan dengan kewajiban mengembalikan harta haram dalam Islam. Kesesuaian pada level jenis dan filosofi sanksi ini menunjukkan bahwa sanksi dalam hukum positif pada dasarnya adalah implementasi modern dari prinsip-prinsip hukuman *ta'zīr*.

4. Legitimasi Hukum Positif dari Perspektif Siyasah Syar'iyyah

Siyāsah Syar'iyyah adalah cabang ilmu fikih yang membahas tentang bagaimana penguasa mengelola negara dan mengatur urusan publik sejalan dengan prinsip-prinsip syariah. Salah satu prinsip utamanya adalah bahwa kebijakan penguasa terhadap rakyatnya harus didasarkan pada kemaslahatan (*taṣarruf al-imām 'alā al-ra'iyyah manūṭun bi al-maṣlaḥah*). Berdasarkan prinsip ini, setiap undang-undang atau kebijakan yang dibuat oleh pemerintah yang bertujuan untuk mewujudkan kemaslahatan hakiki dan menolak kerusakan adalah kebijakan yang sah secara syariah.

Pembuatan dan penegakan hukum positif untuk memberantas kejahatan ekonomi digital adalah contoh nyata dari penerapan *siyāsah syar'iyyah*. Ketika negara mengesahkan UU ITE untuk melindungi warga dari penipuan online, atau UU TPPU untuk menjaga integritas sistem keuangan, tindakan tersebut jelas didasarkan pada pertimbangan kemaslahatan umum. Oleh karena itu, dari perspektif *siyāsah syar'iyyah*, hukum positif tersebut memiliki legitimasi dan ketaatan terhadapnya menjadi sebuah kewajiban.

Pandangan ini menjembatani potensi ketegangan antara "hukum Tuhan" dan "hukum negara". Ia menempatkan hukum negara (selama tidak bertentangan dengan prinsip syariah) sebagai instrumen untuk menegakkan tujuan-tujuan syariah itu sendiri dalam konteks negara

modern. Dengan demikian, seorang Muslim yang taat dapat sekaligus menjadi warga negara yang patuh pada hukum positif, karena keduanya pada akhirnya bertujuan untuk kebaikan bersama.

C. Tantangan dalam Pembuktian (Al-Bayyinah)

Penegakan hukum, baik dalam sistem Islam maupun positif, sangat bergantung pada proses pembuktian (*al-bayyinah*). Kejahatan digital yang bersifat maya dan lintas batas menghadirkan tantangan pembuktian yang unik bagi kedua sistem hukum. Sub-bab ini akan membandingkan alat bukti dalam hukum acara pidana Islam dengan hukum acara modern, membahas penerimaan alat bukti digital dalam fikih kontemporer, dan mengidentifikasi tantangan bersama yang ditimbulkan oleh sifat anonimitas dan transnasional dari kejahatan kripto.

1. Alat Bukti dalam Hukum Acara Pidana Islam (Syahadah, Iqrar, dll.)

Hukum acara pidana Islam mengenal beberapa jenis alat bukti utama yang memiliki kekuatan pembuktian yang berbeda-beda. Alat bukti yang paling kuat adalah pengakuan (*iqrār*) dari pelaku, yang dianggap sebagai "raja dari segala bukti" (*sayyid al-adillah*). Selanjutnya adalah kesaksian (*syahādah*), yang memerlukan sejumlah saksi yang adil dan memenuhi syarat-syarat ketat, terutama untuk kejahatan *hudūd*. Alat bukti lainnya termasuk sumpah (*al-yamīn*) dan penolakannya (*al-nukūl*), serta pengetahuan hakim (*'ilm al-qāḍī*) yang didasarkan pada keyakinan pribadinya.

Selain itu, ada kategori alat bukti yang disebut *qarīnah*, yaitu indikasi atau bukti tidak langsung yang dapat digunakan untuk mendukung atau memperkuat keyakinan hakim. *Qarīnah* bisa berupa jejak kaki, barang bukti yang ditemukan di TKP, atau hasil analisis forensik. Dalam kasus-kasus *ta'zīr*, di mana syarat pembuktian tidak seketat *hudūd*, peran *qarīnah* menjadi sangat penting dan sering kali menjadi dasar utama putusan hakim.

Kekuatan sistem pembuktian Islam terletak pada penekanannya pada kepastian dan keadilan, terutama dalam melindungi terdakwa dari tuduhan palsu melalui syarat saksi yang ketat. Namun, ketergantungan pada bukti-

bukti fisik dan kesaksian langsung ini menghadirkan tantangan ketika dihadapkan pada kejahatan siber yang tidak meninggalkan jejak fisik dan pelakunya anonim.

2. Penerimaan Alat Bukti Digital (Qarinah) dalam Fikih Kontemporer

Untuk menjawab tantangan zaman, para ulama dan cendekiawan hukum Islam kontemporer telah melakukan ijtihad mengenai status alat bukti digital. Pandangan yang dominan adalah bahwa alat bukti digital, seperti data transaksi *blockchain*, log server, email, atau rekaman CCTV, dapat diterima sebagai alat bukti yang sah di pengadilan di bawah kategori *qarīnah qāṭi'ah* (indikasi yang sangat kuat atau konklusif). Meskipun bukan *syahādah* atau *iqrār* dalam pengertian klasik, bukti-bukti ini memiliki tingkat objektivitas dan keandalan yang tinggi jika integritasnya dapat dijamin.

Penerimaan ini didasarkan pada argumen bahwa tujuan dari pembuktian adalah untuk mencapai kebenaran materiil dan keyakinan hakim (*ẓann gālib* atau *yaqīn*). Jika sebuah alat bukti baru, yang dimungkinkan oleh teknologi, dapat membantu hakim mencapai keyakinan tersebut dengan tingkat kepastian yang tinggi, maka tidak ada alasan syar'i untuk menolaknya. Analisis forensik digital yang dilakukan oleh seorang ahli yang kompeten dan terpercaya dapat dianalogikan dengan pendapat seorang ahli (*ahl al-khibrah*) yang telah lama diakui dalam tradisi peradilan Islam.

Dengan demikian, terjadi sinkronisasi antara hukum positif (yang secara eksplisit mengakui bukti elektronik melalui UU ITE) dan pandangan fikih kontemporer. Keduanya sama-sama mengakui bahwa jejak digital adalah alat bukti yang valid dan krusial dalam mengadili kejahatan modern. Hal ini memungkinkan proses peradilan yang sejalan dengan prinsip syariah untuk tetap relevan dan efektif di era digital.

3. Tantangan Sifat Anonim dan Lintas Batas (Transnasional)

Meskipun alat bukti digital diterima, kedua sistem hukum menghadapi tantangan bersama yang fundamental: sifat anonim dan lintas batas dari kejahatan *cryptocurrency*. Anonimitas atau pseudonimitas menyulitkan tahap pertama dari setiap investigasi, yaitu atribusi atau identifikasi pelaku. Menghubungkan sebuah alamat dompet kripto dengan identitas seseorang di dunia nyata adalah tantangan teknis yang sangat besar, terutama jika pelaku menggunakan *mixer* atau *privacy coins*.

Tantangan berikutnya adalah sifat transnasional. Seorang peretas di Eropa Timur dapat mencuri aset kripto dari seorang korban di Indonesia melalui server yang berlokasi di negara ketiga. Hal ini menimbulkan masalah yurisdiksi (hukum negara mana yang berlaku?) dan masalah praktis dalam pengumpulan bukti. Penegak hukum Indonesia mungkin perlu meminta data dari bursa atau penyedia layanan internet di negara lain, sebuah proses yang bergantung pada perjanjian bantuan hukum timbal balik (MLA) dan sering kali terhambat oleh birokrasi atau perbedaan sistem hukum.

Tantangan ini bersifat universal dan tidak unik untuk salah satu sistem hukum saja. Baik peradilan berbasis syariah maupun peradilan sekuler sama-sama akan lumpuh jika tidak mampu mengidentifikasi pelaku atau mengumpulkan bukti dari luar negeri. Ini menegaskan bahwa solusi untuk kejahatan siber tidak bisa hanya bersifat hukum, tetapi juga harus bersifat teknis dan diplomatik, menuntut adanya kerja sama internasional yang erat dan standar global untuk berbagi data lintas batas.

4. Perlunya Ahli Forensik Digital dalam Proses Peradilan Islam

Menghadapi kompleksitas teknis ini, peran ahli (*ahl al-khibrah*) menjadi sangat vital dalam proses peradilan modern yang ingin sejalan dengan prinsip Islam. Dalam kasus kejahatan *cryptocurrency*, hakim yang mungkin tidak memiliki latar belakang teknis akan sangat bergantung pada kesaksian dan laporan dari ahli forensik digital. Ahli inilah yang dapat "menerjemahkan" data *blockchain* yang rumit menjadi narasi yang dapat dipahami, menjelaskan cara kerja sebuah serangan peretasan, atau memverifikasi keaslian sebuah bukti digital.

Dalam tradisi fikih, pendapat seorang ahli yang adil dan kompeten di bidangnya memiliki bobot yang kuat dan dapat menjadi dasar bagi putusan hakim, terutama dalam masalah-masalah teknis. Oleh karena itu, pengembangan kapasitas sumber daya manusia di bidang forensik digital yang tidak hanya kompeten secara teknis tetapi juga memiliki integritas moral (bersifat *'adil*) menjadi sebuah keharusan. Lembaga peradilan, baik di lingkungan peradilan umum maupun peradilan agama (jika diberi kewenangan), perlu memiliki akses ke ahli-ahli semacam ini.

Integrasi keahlian teknis modern ke dalam kerangka peradilan Islam bukanlah sebuah bid'ah, melainkan sebuah keniscayaan untuk memastikan bahwa keadilan dapat ditegakkan secara efektif di zaman sekarang. Tanpa bantuan para ahli forensik digital, hakim akan kesulitan untuk mencapai tingkat keyakinan yang diperlukan untuk menghukum pelaku, yang pada akhirnya dapat menyebabkan para penjahat siber lolos dari jerat hukum dan tujuan syariah untuk melindungi masyarakat tidak tercapai.

D. Mekanisme Perampasan Aset Hasil Kejahatan

Salah satu tujuan utama dari peradilan pidana dalam kejahatan ekonomi adalah untuk memastikan bahwa "kejahatan tidak menghasilkan keuntungan" (*crime doesn't pay*). Sub-bab ini akan membandingkan mekanisme perampasan aset dalam hukum positif Indonesia, khususnya UU TPPU, dengan konsep pengembalian harta haram dalam fikih Islam. Akan dibahas pula keselarasan dalam pemanfaatan aset rampasan dan tantangan teknis yang spesifik dalam merampas aset kripto.

1. Konsep Pengembalian Harta Haram dalam Islam

Hukum Islam memiliki prinsip yang sangat jelas mengenai harta yang diperoleh dari cara yang tidak sah (*ḥarām*): harta tersebut tidak menjadi hak milik pelaku dan harus dikembalikan. Prinsip ini didasarkan pada hadis Nabi yang menyatakan, "Atas tangan (yang mengambil), ada kewajiban untuk mengembalikan apa yang telah diambilnya hingga ia mengembalikannya." Ini berarti, prioritas utama setelah sebuah kejahatan harta terbukti adalah restitusi, yaitu mengembalikan harta tersebut kepada pemiliknya yang sah.

Jika pemiliknya yang sah tidak dapat ditemukan atau diidentifikasi (misalnya, dalam kasus di mana korbannya sangat banyak dan tersebar), maka harta haram tersebut harus diserahkan kepada kas negara (*bayt al-māl*) untuk digunakan bagi kemaslahatan umum. Pelaku kejahatan sama sekali tidak berhak untuk menikmati atau bahkan menyedekahkan harta tersebut atas namanya sendiri, karena ia bukan pemiliknya. Kewajiban untuk membersihkan diri dari harta haram ini bersifat mutlak.

Konsep ini menunjukkan bahwa fokus hukum Islam tidak hanya pada penghukuman pelaku (*retribusi*), tetapi juga sangat kuat pada pemulihan hak korban (*restorasi*). Tujuan peradilan tidak tercapai sepenuhnya jika

pelaku hanya dipenjara sementara hasil kejahatannya masih bisa dinikmati olehnya atau keluarganya. Harta tersebut harus dirampas dan dikembalikan ke tempatnya yang semestinya.

2. Perampasan Aset dalam UU TPPU dan Kesesuaiannya dengan Fikih

Mekanisme perampasan aset dalam hukum positif Indonesia, terutama yang diatur dalam UU TPPU, menunjukkan keselarasan yang luar biasa dengan konsep fikih ini. UU TPPU memungkinkan negara untuk melakukan penyitaan dan perampasan terhadap seluruh aset yang merupakan hasil tindak pidana atau yang terkait dengan pencucian uang. Tujuannya adalah untuk memiskinkan para pelaku kejahatan dan mengembalikan kerugian negara atau masyarakat.

Pendekatan "ikuti jejak uang" (*follow the money*) yang menjadi inti dari UU TPPU adalah implementasi modern dari prinsip pelacakan dan pengembalian harta haram. Ketika PPATK dan penegak hukum melacak aliran dana kripto dari sebuah penipuan, membekukannya di bursa, dan kemudian pengadilan memutuskan untuk merampasnya, proses tersebut secara substansial adalah pelaksanaan dari kewajiban untuk mengambil kembali harta yang diperoleh secara batil.

Lebih lanjut, UU TPPU juga mengenal konsep perampasan aset tanpa pemidanaan (*non-conviction based asset forfeiture*) dalam kondisi tertentu, misalnya jika terdakwa meninggal dunia atau melarikan diri. Hal ini juga sejalan dengan prinsip fikih bahwa status haram melekat pada hartanya itu sendiri, terlepas dari apakah pelakunya berhasil dihukum atau tidak. Keselarasan ini menunjukkan bahwa mekanisme perampasan aset dalam hukum positif merupakan instrumen yang sangat efektif dan sejalan dengan syariah untuk mencapai keadilan ekonomi.

3. Pemanfaatan Aset Rampasan untuk Kemaslahatan Umum (Baitul Mal)

Setelah aset dirampas, pertanyaan selanjutnya adalah untuk apa aset tersebut digunakan. Seperti yang telah disebutkan, fikih Islam mengarahkan agar aset rampasan yang pemiliknya tidak diketahui diserahkan ke *bayt al-māl* untuk kemaslahatan umum. Ini bisa berarti membiayai pendidikan, kesehatan, infrastruktur, atau program pengentasan kemiskinan. Tujuannya

adalah agar harta yang semula digunakan untuk keburukan dapat diubah menjadi sumber kebaikan bagi masyarakat luas.

Hukum positif Indonesia memiliki mekanisme yang serupa. Aset hasil kejahatan yang dirampas oleh negara akan menjadi milik negara dan masuk ke dalam kas negara. Pengelolaannya kemudian diatur melalui mekanisme APBN untuk membiayai berbagai program pembangunan dan pelayanan publik. Dalam beberapa kasus, undang-undang juga memungkinkan agar aset rampasan secara spesifik dialokasikan untuk upaya penegakan hukum atau untuk memberikan kompensasi kepada korban kejahatan.

Konvergensi dalam prinsip pemanfaatan aset rampasan ini sangat penting. Keduanya sama-sama menolak gagasan bahwa aset tersebut menjadi hak milik aparat atau pejabat yang menyitanya. Sebaliknya, aset tersebut harus kembali kepada publik dalam bentuk pelayanan atau program yang bermanfaat. Ini menegaskan kembali bahwa tujuan akhir dari penegakan hukum adalah untuk mewujudkan kemaslahatan umum, sebuah prinsip yang dijunjung tinggi oleh kedua sistem hukum.

4. Tantangan Teknis dalam Merampas Aset Kripto

Meskipun prinsipnya selaras, perampasan aset kripto menghadirkan tantangan teknis yang tidak ada pada aset konvensional. Tantangan terbesar adalah penguasaan *private key*. Aset kripto tidak dapat disita atau dipindahkan tanpa akses ke *private key* dari dompet yang menyimpannya. Jika pelaku menyimpan asetnya di *non-custodial wallet* (misalnya, *hardware wallet*) dan menolak untuk menyerahkan *private key*-nya, penegak hukum akan menghadapi jalan buntu.

Untuk mengatasi ini, penegak hukum harus mengembangkan kemampuan teknis dan investigatif untuk menemukan *private key* atau *seed phrase* yang mungkin disembunyikan oleh pelaku, baik dalam bentuk digital maupun fisik. Ini bisa melibatkan analisis forensik mendalam terhadap perangkat elektronik pelaku atau teknik interogasi yang efektif. Dalam beberapa kasus, negara bahkan mungkin perlu menggunakan ancaman sanksi pidana tambahan (seperti penghinaan terhadap pengadilan) untuk memaksa pelaku menyerahkan kuncinya.

Tantangan lainnya adalah volatilitas harga. Nilai aset kripto yang disita dapat berubah secara drastis selama proses hukum berlangsung. Hal ini menimbulkan pertanyaan mengenai manajemen aset sitaan: haruskah aset tersebut segera dilikuidasi menjadi uang fiat, atau harus disimpan dalam bentuk kripto hingga putusan pengadilan berkekuatan hukum tetap? Diperlukan adanya peraturan teknis dan infrastruktur yang memadai bagi lembaga pengelola barang sitaan (seperti Rupbasan) untuk dapat menangani aset digital secara aman dan efektif.

E. Potensi Adopsi Nilai-Nilai Hukum Pidana Islam dalam Pembaharuan Hukum Nasional

Harmonisasi bukan hanya tentang mencari kesamaan, tetapi juga tentang bagaimana satu sistem dapat belajar dan mengadopsi nilai-nilai terbaik dari sistem lain. Sub-bab terakhir ini akan mengeksplorasi bagaimana nilai-nilai dan prinsip-prinsip dari hukum pidana Islam dapat memberikan inspirasi bagi pembaharuan hukum pidana nasional di Indonesia, khususnya dalam menghadapi kejahatan ekonomi digital. Fokus akan diberikan pada penguatan efek jera, keadilan restoratif, fleksibilitas sanksi, dan internalisasi etika.

1. Penguatan Efek Jera (Zawajir) dalam Sanksi Pidana

Filsafat pemidanaan dalam Islam sangat menekankan fungsi *zawājir*, yaitu pencegahan atau efek jera. Hukuman tidak hanya bertujuan untuk membalas perbuatan pelaku, tetapi juga untuk menjadi pelajaran yang sangat kuat bagi masyarakat agar tidak melakukan kejahatan serupa. Sanksi yang berat dan tegas untuk kejahatan-kejahatan besar seperti *ḥirābah* mencerminkan prinsip ini. Dalam konteks kejahatan ekonomi digital yang merugikan ribuan korban dan merusak kepercayaan publik, semangat *zawājir* ini sangat relevan.

Pembaharuan hukum nasional dapat mengadopsi semangat ini dengan merancang sanksi yang benar-benar memberikan efek jera bagi para pelaku kejahatan kerah putih dan siber. Ini bisa berarti hukuman penjara minimum yang lebih tinggi untuk penipuan skala besar, denda yang bersifat multikelipatan dari keuntungan yang diperoleh, serta penerapan sanksi tambahan seperti pencabutan hak untuk menjalankan usaha di

sektor keuangan seumur hidup. Tujuannya adalah untuk mengirimkan pesan yang jelas bahwa kejahatan ekonomi digital adalah kejahatan serius dengan konsekuensi yang sangat berat.

Selain itu, konsep *tashhīr* (mempublikasikan identitas dan kejahatan pelaku) dapat diadopsi secara lebih sistematis. Meskipun sudah ada dalam bentuk pengumuman putusan hakim, penerapannya dapat diperluas. Mempublikasikan daftar para penipu investasi atau peretas yang telah dihukum dapat menjadi alat pencegahan yang efektif, karena sanksi sosial dan reputasi sering kali sama ditakutinya dengan sanksi finansial atau kurungan.

2. Prinsip Keadilan Restoratif (Ishlah) dan Ganti Rugi Korban

Di samping ketegasan, hukum pidana Islam juga memiliki sisi restoratif yang kuat, yang terangkum dalam konsep *iṣlāḥ* (perbaikan) dan penekanan pada pemulihan hak korban. Dalam kejahatan *qiṣāṣ-diyat*, hak korban atau keluarganya untuk memaafkan atau menerima kompensasi (*diyat*) sangat diutamakan. Dalam kejahatan harta, pengembalian aset curian adalah prioritas utama. Semangat keadilan restoratif ini dapat diadopsi lebih kuat dalam sistem peradilan pidana nasional.

Saat ini, fokus utama peradilan pidana sering kali adalah pada hubungan antara negara dan pelaku, sementara korban sering kali terpinggirkan. Pembaharuan hukum dapat memperkuat mekanisme restitusi (ganti rugi yang dibebankan pada pelaku) dan kompensasi (ganti rugi yang diberikan oleh negara jika pelaku tidak mampu). Proses mediasi antara pelaku dan korban, terutama dalam kasus-kasus yang tidak terlalu berat, juga dapat dieksplorasi sebagai alternatif penyelesaian perkara yang lebih memulihkan.

Dalam kasus penipuan investasi kripto, misalnya, proses hukum harus secara proaktif bertujuan untuk mengembalikan dana korban semaksimal mungkin, bukan hanya memenjarakan pelakunya. Pengadilan dapat didorong untuk mengeluarkan putusan yang inovatif, seperti memerintahkan pelaku untuk bekerja dan penghasilannya digunakan untuk mencicil ganti rugi kepada para korban. Ini sejalan dengan semangat *iṣlāḥ* yang bertujuan untuk memperbaiki kerusakan yang telah terjadi.

3. Fleksibilitas Hukuman Ta'zir untuk Kasus yang Beragam

Salah satu keunggulan terbesar dari sistem sanksi *ta'zīr* adalah fleksibilitasnya yang luar biasa. Hakim memiliki palet hukuman yang sangat luas dan dapat menyesuaikannya dengan karakteristik unik dari setiap kasus dan setiap pelaku. Prinsip ini dapat menginspirasi pembaharuan hukum acara pidana untuk memberikan diskresi yang lebih terarah kepada hakim, menjauhi kekakuan positivisme legalistik yang terkadang menghasilkan putusan yang tidak adil.

Kejahatan ekonomi digital memiliki spektrum yang sangat luas, mulai dari seorang remaja yang iseng melakukan peretasan kecil hingga sindikat internasional yang mencuci uang miliaran dolar. Menyamaratakan hukuman untuk spektrum yang begitu lebar tentu tidak adil. Semangat fleksibilitas *ta'zīr* mendorong adanya pedoman pemidanaan (*sentencing guidelines*) yang lebih canggih, yang membantu hakim mempertimbangkan berbagai faktor seperti tingkat kerugian, peran pelaku (otak intelektual vs. pelaku lapangan), tingkat kecanggihan teknis, dan apakah pelaku menunjukkan penyesalan dan bekerja sama untuk memulihkan kerugian.

Selain itu, fleksibilitas ini juga memungkinkan adanya sanksi-sanksi alternatif yang lebih kreatif dan mendidik selain penjara dan denda. Misalnya, seorang peretas muda yang berbakat dapat dihukum dengan kerja sosial di mana ia harus menggunakan keahliannya untuk membantu memperkuat sistem keamanan siber lembaga pemerintah atau nirlaba. Hukuman semacam ini tidak hanya menghukum, tetapi juga merehabilitasi dan mengubah potensi destruktif menjadi kontribusi positif, sebuah pendekatan yang sangat sejalan dengan tujuan pemidanaan dalam Islam.

4. Internalisasi Nilai Etika dan Moral Islam dalam Regulasi Ekonomi Digital

Terakhir, harmonisasi tidak hanya terjadi pada level hukum pidana (*penindakan*), tetapi juga dapat terjadi pada level regulasi dan pencegahan. Hukum Islam, khususnya fikih muamalah, kaya akan prinsip-prinsip etika dan moral yang dapat diinternalisasi dalam penyusunan regulasi ekonomi digital. Prinsip-prinsip seperti larangan *gharar* (ketidakpastian

yang berlebihan), *maysir* (spekulasi/perjudian), *tadlis* (penipuan informasi), dan keharusan adanya transparansi dapat menjadi landasan filosofis bagi regulasi yang lebih adil dan melindungi konsumen.

Misalnya, regulasi Bappebti atau OJK di masa depan dapat secara eksplisit mewajibkan setiap proyek aset kripto yang ingin terdaftar di Indonesia untuk menyediakan *whitepaper* yang sangat jelas, transparan, dan tidak mengandung janji-janji yang menyesatkan. Kewajiban untuk melakukan audit keamanan *smart contract* oleh pihak ketiga yang independen dapat dipandang sebagai implementasi modern dari upaya menghilangkan *gharar* teknis. Regulasi yang melarang iklan investasi kripto yang terlalu bombastis dan tidak menyertakan peringatan risiko yang jelas adalah bentuk konkret dari pencegahan *tadlis*.

Dengan menginternalisasi nilai-nilai etika ini ke dalam "DNA" regulasi, negara tidak hanya bertindak sebagai penegak hukum di hilir, tetapi juga sebagai pembentuk ekosistem yang sehat di hulu. Ini adalah pendekatan preventif yang sejalan dengan kaidah *sadd al-żarī'ah* (menutup jalan menuju keburukan). Menciptakan sebuah industri ekonomi digital yang tidak hanya patuh hukum, tetapi juga beretika dan bermoral, adalah tujuan jangka panjang yang dapat dicapai melalui sinergi antara kearifan hukum Islam dan instrumen regulasi modern.

Analisis Mendalam Konsep Kunci Bab 7: Sinkronisasi dan Harmonisasi Hukum

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk membangun sebuah jembatan intelektual antara hukum Islam dan hukum nasional. Alih-alih melihatnya sebagai dua sistem yang terpisah atau bahkan berkonflik, bab ini berupaya untuk:

1. Mengidentifikasi Kesamaan Filosofis: Menemukan nilai-nilai dan tujuan fundamental yang sama (*common ground*) yang mendasari kedua sistem hukum.
2. Mencari Padanan Konseptual: Menunjukkan bagaimana konsep-konsep kunci dalam hukum pidana Islam memiliki padanan fungsional dalam hukum positif.

3. Menganalisis Tantangan Bersama: Mengakui bahwa kedua sistem hukum menghadapi tantangan praktis yang serupa dalam penegakan hukum di era digital.
4. Mengeksplorasi Potensi Adopsi Nilai: Mengusulkan bagaimana nilai-nilai dan prinsip-prinsip dari hukum pidana Islam dapat menginspirasi dan memperkaya pembaharuan hukum nasional di masa depan.

Ini adalah upaya untuk melakukan sintesis, mencari harmoni di tengah perbedaan formal.

Elemen-Elemen Kunci dalam Proses Sinkronisasi:

1. Level Filosofis (Tujuan Hukum): Membandingkan *Maqashid al-Shari'ah* dengan tujuan negara hukum Pancasila.
2. Level Konseptual (Kewenangan & Delik): Membandingkan konsep *Ta'zir* dengan kewenangan legislasi negara, dan delik-delik spesifik.
3. Level Praktis (Pembuktian & Eksekusi): Membandingkan tantangan dalam hukum acara kedua sistem.
4. Level Visioner (Pembaharuan Hukum): Melihat bagaimana satu sistem dapat belajar dari yang lain.

Analisis Komparatif: Titik Temu Hukum Islam dan Hukum Positif

Tabel berikut memetakan proses sinkronisasi dan harmonisasi antara kedua sistem hukum dalam menanggulangi kejahatan ekonomi digital.

Aspek Perbandingan	Hukum Pidana Islam (Perspektif Fikih Jinayah)	Hukum Positif Indonesia	Titik Temu dan Harmonisasi
1. Tujuan Fundamental (Filosofi)	Maqashid al-Shari'ah: Melindungi lima nilai universal: agama (*din*), jiwa (*nafs*), akal (*'aql*), keturunan (*nasl*), dan harta (*maal*).	Tujuan Negara (UUD 1945): Melindungi segenap bangsa, memajukan kesejahteraan umum, dan menciptakan ketertiban umum.	Konvergensi pada Kemaslahatan Publik. Keduanya bertujuan melindungi warga negara dari kerugian (perlindungan harta), menjaga keamanan (perlindungan jiwa), dan memelihara ketertiban sosial.
2. Sumber Kewenangan Mengatur Kejahatan Baru	Kewenangan *Ulil Amr* dalam *Jarimah Ta'zir*. Pemerintah berhak membuat aturan pidana baru demi kemaslahatan umum.	Kewenangan Legislatif (DPR & Pemerintah). Berdasarkan konstitusi, negara berhak membentuk undang-undang untuk mengatur kehidupan berbangsa.	Padanan Fungsional. Kewenangan legislasi negara dalam hukum positif dapat dipandang sebagai manifestasi modern dari konsep kewenangan *ulil amr* dalam menetapkan *jarimah ta'zir*.
3. Kualifikasi Kejahatan (Contoh: Penipuan)	Dikualifikasikan sebagai *Jarimah Ta'zir* karena melanggar larangan memakan harta secara batil dan mengandung unsur *tadlis* (penipuan).	Dikualifikasikan sebagai Tindak Pidana Penipuan (Pasal 378 KUHP) karena mengandung unsur "tipu muslihat" dan "rangkaian kebohongan".	Kesamaan Esensi. Meskipun istilahnya berbeda, keduanya sama-sama fokus pada esensi perbuatan: mengambil harta orang lain dengan cara yang tidak benar. UU ITE dan UU TPPU adalah bentuk *ta'zir* modern.

Aspek Perbandingan	Hukum Pidana Islam (Perspektif Fikih Jinayah)	Hukum Positif Indonesia	Titik Temu dan Harmonisasi
4. Pembuktian di Era Digital	Menghadapi tantangan dalam menerapkan alat bukti klasik (*syahadah, iqrar*). Namun, membuka ruang untuk bukti petunjuk (*qarinah*) yang kuat, seperti jejak digital.	Mengakui alat bukti elektronik secara eksplisit melalui UU ITE (Pasal 5), yang merupakan perluasan dari alat bukti dalam KUHAP.	Tantangan Bersama & Solusi Serupa. Keduanya menghadapi kesulitan atribusi pelaku anonim. Keduanya juga sama-sama menerima bukti digital sebagai alat bukti yang sah dan kuat (*qarinah qath'iyyah*).
5. Sanksi dan Pemidanaan	Sanksi Ta'zir sangat fleksibel, mencakup penjara, denda, ganti rugi, hingga publikasi, dengan tujuan utama perbaikan (*ishlah*) dan pencegahan (*zawajir*).	Sanksi dalam KUHP dan UU lainnya mencakup penjara, denda, dan hukuman tambahan. Fokus utama sering kali pada retribusi dan penjeraan.	Potensi Sinergi. Fleksibilitas *ta'zir* dan penekanannya pada keadilan restoratif (pemulihan korban) dapat menginspirasi pembaharuan hukum pidana positif agar tidak terlalu kaku dan lebih berorientasi pada korban.

Kontribusi Konsep Sinkronisasi dalam Bab 7:

Konsep ini adalah puncak dari argumen komparatif buku ini.

1. Membangun Jembatan, Bukan Tembok: Bab ini secara eksplisit menolak pandangan yang mempertentangkan hukum Islam dengan hukum negara. Sebaliknya, ia menunjukkan bahwa keduanya dapat dan seharusnya saling mengisi.
2. Memberikan Dimensi Spiritual pada Hukum Positif: Dengan menunjukkan kesamaan tujuan antara hukum positif dan *Maqashid al-Shari'ah*, bab ini memberikan "ruh" atau dimensi spiritual pada penegakan hukum positif. Penegakan UU TPPU, misalnya, bukan hanya tugas negara, tetapi juga sebuah implementasi dari prinsip *hifzh al-maal* (menjaga harta).
3. Menawarkan Arah Pembaharuan Hukum: Ini adalah kontribusi paling visioner dari bab ini. Ia tidak hanya menganalisis apa yang ada, tetapi juga mengusulkan "apa yang seharusnya". Konsep keadilan restoratif, fleksibilitas sanksi, dan penguatan ganti rugi korban dari fikih jinayah ditawarkan sebagai "bahan" berharga untuk menyempurnakan Kitab Undang-Undang Hukum Pidana (KUHP) nasional yang baru.

Secara ringkas, Bab 7 berperan sebagai seorang "diplomat" yang mendamaikan dan mencari sinergi antara dua tradisi hukum yang besar. Ia berargumen bahwa untuk menghadapi tantangan sekompleks kejahatan digital, Indonesia tidak perlu memilih salah satu, melainkan dapat memanfaatkan kearifan dari kedua sistem hukum tersebut secara harmonis.

BAB 8

Potter Kasus Kejahatan Cryptocurrency di Indonesia (Analisis Yuridis)

Setelah memetakan kerangka hukum pidana Islam dan hukum positif serta potensi harmonisasinya, Bagian IV dari buku ini beralih ke ranah implementasi praktis. Bab 8 secara khusus akan menguji teori dan peraturan yang telah dibahas dengan menganalisisnya melalui lensa studi kasus konkret yang terjadi di Indonesia. Analisis kasus adalah metode krusial untuk memahami bagaimana hukum bekerja dalam praktik, mengidentifikasi di mana letak kekuatannya, dan di mana ia masih menunjukkan kelemahan. Dengan membedah kasus-kasus yang telah menarik perhatian publik, kita dapat melihat secara langsung bagaimana aparat penegak hukum—mulai dari penyidik, jaksa, hingga hakim—bergulat dengan kompleksitas kejahatan ekonomi digital. *Research gap* yang diisi oleh bab ini adalah kurangnya analisis yuridis yang sistematis dan komparatif terhadap berbagai jenis kasus kejahatan kripto di Indonesia dalam satu pembahasan terpadu. Pertanyaan penelitian utama bab ini adalah: Bagaimana penegak hukum Indonesia menerapkan instrumen hukum positif dalam menangani kasus penipuan, pencucian uang, dan kejahatan lain yang melibatkan *cryptocurrency*, dan pelajaran apa yang dapat dipetik dari putusan-putusan pengadilan yang ada untuk perbaikan penegakan hukum di masa depan?

A. Kasus Penipuan Investasi Robot Trading (Contoh: Fahrenheit/Net89)

Kasus penipuan berkedok investasi robot trading, seperti Fahrenheit dan Net89, merupakan salah satu skandal keuangan digital terbesar di Indonesia yang merugikan ribuan korban dengan total kerugian triliunan rupiah. Meskipun tidak secara langsung menggunakan *cryptocurrency* sebagai produk utama, kasus ini sering kali melibatkan aset kripto dalam mekanisme operasional dan pencucian uangnya. Sub-bab ini akan membedah kronologi kasus, dakwaan jaksa, putusan hakim, dan analisis terhadap efektivitas penegakan hukum.

1. Kronologi dan Modus Operandi Kasus

Modus operandi kasus Fahrenheit dan sejenisnya pada dasarnya adalah skema Ponzi yang dibalut dengan teknologi canggih. Pelaku menawarkan produk investasi berupa penyewaan "robot trading" yang diklaim dapat menghasilkan keuntungan konsisten dan sangat tinggi (misalnya, 1-2%

per hari) dari perdagangan di pasar valuta asing atau komoditas. Untuk menarik korban, para pelaku membangun narasi tentang kecanggihan teknologi *Artificial Intelligence* (AI) dan menampilkan gaya hidup mewah yang didanai dari "keuntungan" trading. Pemasaran dilakukan secara masif melalui seminar-seminar megah, media sosial, dan dengan merekrut *influencer* serta figur publik sebagai afiliator.

Para korban diwajibkan untuk menyetor sejumlah dana (sering kali dalam bentuk Dolar AS yang ditransfer melalui perantara atau dikonversi menjadi aset kripto seperti USDT) ke akun yang dikelola oleh perusahaan. Pada awalnya, sistem menunjukkan keuntungan yang dijanjikan di dasbor akun korban, dan beberapa investor awal bahkan dapat melakukan penarikan dana. Mekanisme ini klasik dalam skema Ponzi, di mana dana dari investor baru digunakan untuk membayar "keuntungan" investor lama, sehingga menciptakan ilusi profitabilitas dan memicu promosi dari mulut ke mulut.

Keruntuhan terjadi ketika jumlah investor baru tidak lagi mencukupi untuk menutupi permintaan penarikan dana. Pada titik ini, perusahaan tiba-tiba menghentikan layanan penarikan dengan berbagai alasan, seperti "pemeliharaan sistem", "serangan peretas", atau "kondisi pasar yang buruk". Akhirnya, para pelaku menghilang bersama sisa dana investor yang terkumpul, meninggalkan kerugian masif. Sebagian dana tersebut dilarikan ke luar negeri atau dicuci melalui pembelian aset-aset mewah dan *cryptocurrency* untuk menyamarkan jejaknya.

2. Dakwaan Jaksa: Penerapan Pasal KUHP, UU Perdagangan, dan UU TPPU

Dalam menghadapi kasus-kasus ini, jaksa penuntut umum biasanya menggunakan dakwaan berlapis (kumulatif) untuk memastikan pelaku dapat dijerat dari berbagai sisi. Dakwaan pertama umumnya menggunakan Pasal 378 KUHP tentang Penipuan, dengan argumen bahwa pelaku telah menggunakan "rangkaian kebohongan" (janji keuntungan tidak realistis) untuk menggerakkan korban menyerahkan uangnya. Dakwaan ini sering kali digabungkan dengan Pasal 372 KUHP tentang Penggelapan, dengan argumen bahwa pelaku telah menyalahgunakan dana yang dipercayakan oleh para investor.

Dakwaan kedua yang sangat penting adalah dari Undang-Undang No. 7 Tahun 2014 tentang Perdagangan. Pelaku dijerat dengan pasal yang melarang praktik skema piramida dalam distribusi barang atau jasa. Jaksa berargumen bahwa sistem bonus afiliasi yang masif, di mana anggota mendapatkan keuntungan lebih besar dari merekrut anggota baru daripada dari hasil trading itu sendiri, adalah ciri khas skema piramida. Selain itu, pelaku juga dijerat karena menjalankan usaha perdagangan tanpa memiliki izin yang sah dari Bappebti.

Dakwaan ketiga, yang berfungsi sebagai pamungkas, adalah Undang-Undang No. 8 Tahun 2010 tentang TPPU. Jaksa menuntut pelaku dengan tindak pidana pencucian uang karena mereka telah secara aktif menyembunyikan, mentransfer, dan mengubah bentuk hasil kejahatan penipuan dan perdagangan ilegal tersebut menjadi aset lain (rumah, mobil mewah, jam tangan, termasuk aset kripto) untuk menyamarkan asal-usulnya. Penggunaan dakwaan TPPU ini krusial untuk memungkinkan perampasan aset pelaku.

3. Putusan Hakim dan Pertimbangan Hukumnya

Dalam banyak kasus robot trading, majelis hakim pada akhirnya sependapat dengan dakwaan jaksa dan menyatakan para terdakwa terbukti secara sah dan meyakinkan melakukan tindak pidana penipuan, perdagangan ilegal, dan pencucian uang secara bersama-sama. Pertimbangan hukum hakim biasanya menekankan pada terpenuhinya unsur "tipu muslihat" dalam Pasal 378 KUHP, yang dibuktikan dari kesaksian para korban dan bukti-bukti digital berupa promosi yang menyesatkan. Hakim juga mengakui bahwa model bisnis yang dijalankan adalah skema piramida yang dilarang oleh UU Perdagangan.

Salah satu aspek yang paling krusial dalam putusan adalah terkait perampasan aset. Hakim, berdasarkan dakwaan TPPU, akan memerintahkan agar seluruh aset yang terbukti berasal dari hasil kejahatan dirampas. Namun, perdebatan hukum yang sengit sering kali terjadi mengenai status aset rampasan tersebut: apakah harus dikembalikan kepada para korban atau dirampas untuk negara? Dalam beberapa putusan, hakim memutuskan aset dirampas untuk negara, dengan pertimbangan bahwa sulit untuk mengidentifikasi dan memverifikasi semua korban serta menghitung

kerugian secara proporsional. Putusan ini sering kali menimbulkan kekecewaan di pihak korban yang berharap dana mereka dapat kembali.

Putusan hakim dalam kasus-kasus ini menunjukkan bahwa pengadilan telah mengakui kejahatan skema Ponzi digital sebagai kejahatan serius. Vonis hukuman penjara yang dijatuhkan kepada para petingginya, yang bisa mencapai belasan tahun, ditambah dengan perampasan seluruh aset, mengirimkan sinyal efek jera yang kuat. Namun, isu mengenai pengembalian aset kepada korban tetap menjadi pekerjaan rumah yang kompleks bagi sistem peradilan pidana.

4. Analisis Kelemahan dan Kekuatan Penegakan Hukum

Kekuatan utama penegakan hukum dalam kasus ini adalah kemampuan penyidik dan jaksa untuk menggunakan pendekatan multi-undang-undang (*multi-door approach*). Kombinasi KUHP, UU Perdagangan, dan UU TPPU terbukti menjadi formula yang efektif untuk menjerat pelaku dari berbagai aspek perbuatan mereka. Khususnya, penggunaan UU TPPU sangat vital karena memungkinkan pelacakan dan perampasan aset, yang merupakan inti dari penegakan hukum terhadap kejahatan ekonomi. Kolaborasi antara Bareskrim Polri dan PPATK juga menjadi kunci keberhasilan dalam menelusuri aliran dana.

Namun, beberapa kelemahan juga terlihat jelas. Pertama, penegakan hukum sering kali bersifat reaktif, baru bergerak setelah skema tersebut runtuh dan ribuan orang menjadi korban. Upaya pencegahan dari sisi regulator (OJK dan Bappebti) melalui Satgas Waspada Investasi sering kali kalah cepat dengan masifnya pemasaran para pelaku. Kedua, proses hukum yang panjang dan kompleks, ditambah dengan kesulitan dalam melacak aset yang sudah dilarikan ke luar negeri, membuat pemulihan aset (*asset recovery*) menjadi tidak maksimal.

Kelemahan ketiga, seperti yang telah disinggung, adalah dilema dalam distribusi aset rampasan. Belum adanya mekanisme yang baku dan efisien untuk mengelola dan mendistribusikan aset sitaan kepada ribuan korban dalam kasus penipuan massal menjadi tantangan yuridis dan teknis. Hal ini menunjukkan perlunya pembaharuan dalam hukum acara pidana atau pembuatan peraturan khusus yang mengatur tentang restitusi bagi korban kejahatan massal.

B. Kasus Pencucian Uang oleh Influencer (Contoh: Doni Salmanan)

Kasus yang menjerat *influencer* Doni Salmanan menyoroti persimpangan antara platform investasi ilegal (*binary option*), peran *influencer* sebagai afiliator, dan penggunaan aset kripto sebagai salah satu metode untuk menikmati hasil kejahatan. Meskipun kejahatan utamanya terkait dengan platform Quotex (*binary option*), kasus ini memberikan pelajaran penting tentang pencucian uang di era digital. Sub-bab ini akan menganalisis keterkaitan kasus dengan kripto, penerapan UU ITE dan TPPU, serta proses pelacakan asetnya.

1. Keterkaitan Kasus dengan Aset Kripto

Dalam kasus Doni Salmanan, kejahatan utamanya adalah menjadi afiliator platform *binary option* Quotex, yang dianggap sebagai perjudian berkedok trading. Ia secara aktif menyebarkan berita bohong melalui kanal YouTube-nya, mengklaim bahwa ia berhasil meraup keuntungan fantastis dari platform tersebut, dan mengajak para pengikutnya untuk bergabung menggunakan kode referalnya. Keuntungan yang ia peroleh sebagian besar berasal dari komisi atas kerugian para anggota yang direkrutnya.

Keterkaitan dengan aset kripto muncul dalam fase pencucian uang. Setelah menerima keuntungan ilegal dari Quotex (sering kali dalam bentuk mata uang digital atau transfer internasional), Doni Salmanan kemudian mengonversi dan membelanjakan dana tersebut untuk membeli berbagai aset mewah, termasuk mobil sport, motor gede, dan properti. Selain itu, ia juga diketahui melakukan transaksi jual beli aset kripto di bursa domestik. Tindakan ini merupakan upaya untuk menyamarkan asal-usul uang yang diperolehnya dari aktivitas ilegal sebagai afiliator.

Meskipun bukan inti kejahatan, penggunaan aset kripto dalam portofolio pencucian uangnya menunjukkan bagaimana para pelaku kejahatan modern memanfaatkan berbagai instrumen keuangan digital untuk mengaburkan jejak dana mereka. Mereka tidak hanya bergantung pada sistem perbankan konvensional, tetapi juga merambah ke ekosistem aset digital untuk menempatkan dan melapis (*layering*) hasil kejahatan mereka.

2. Penerapan UU ITE dan UU TPPU

Dakwaan terhadap Doni Salmanan berpusat pada dua undang-undang utama. Pertama, Pasal 45A ayat (1) jo. Pasal 28 ayat (1) UU ITE. Jaksa berargumen bahwa ia telah dengan sengaja menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. "Berita bohong" tersebut adalah klaim bahwa *binary option* adalah trading yang menguntungkan, padahal pada dasarnya adalah perjudian di mana afiliator diuntungkan dari kerugian pemain. "Kerugian konsumen" adalah dana yang hilang oleh para pengikutnya di platform Quotex.

Kedua, dan yang paling signifikan, adalah dakwaan Pasal 3 UU TPPU tentang Tindak Pidana Pencucian Uang. Jaksa menuduh bahwa Doni Salmanan telah secara aktif mentransfer, membelanjakan, dan mengubah bentuk harta kekayaan yang ia ketahui atau patut duga berasal dari hasil tindak pidana (dalam hal ini, penyebaran berita bohong menurut UU ITE). Pembelian aset-aset mewah dan transaksi aset kripto yang dilakukannya adalah bagian dari skema pencucian uang ini.

Penerapan kedua undang-undang ini secara bersamaan sangat efektif. UU ITE digunakan untuk menetapkan kejahatan asalnya (*predicate crime*), sementara UU TPPU digunakan untuk menjerat upaya menyembunyikan hasil kejahatan tersebut. Putusan pengadilan, meskipun sempat berliku di tingkat banding sebelum diperbaiki di tingkat kasasi, pada akhirnya menguatkan bahwa perbuatan sebagai afiliator *binary option* adalah tindak pidana dan keuntungan darinya adalah subjek pencucian uang.

3. Proses Pelacakan Aset (*Asset Tracing*) oleh PPATK dan Penyidik

Kasus ini menjadi contoh sukses dari proses pelacakan aset yang dilakukan secara komprehensif oleh PPATK dan Bareskrim Polri. Begitu penyelidikan dimulai, PPATK segera menggunakan kewenangannya untuk membekukan ratusan rekening bank yang terkait dengan Doni Salmanan. Analisis aliran dana (*follow the money*) dilakukan secara mendalam untuk memetakan ke mana saja uang hasil kejahatan itu mengalir.

Proses pelacakan tidak berhenti di sistem perbankan. Penyidik juga menelusuri pembelian aset-aset fisik. Setiap mobil mewah, motor, rumah, dan barang bermerek yang dibeli oleh tersangka selama periode kejahatan

ditelusuri sumber pendanaannya. Jika terbukti dibeli menggunakan uang hasil kejahatan, aset tersebut disita sebagai barang bukti. Ini menunjukkan pendekatan yang tidak hanya fokus pada uang tunai, tetapi pada semua bentuk kekayaan yang merupakan buah dari aktivitas ilegal.

Dalam konteks aset kripto, penyidik bekerja sama dengan bursa kripto domestik tempat tersangka melakukan transaksi. Berdasarkan perintah dari penegak hukum, bursa akan memberikan data riwayat transaksi dan membekukan sisa saldo yang ada di akun tersangka. Meskipun mungkin tidak semua aset kriptonya dapat dilacak (terutama jika ada yang disimpan di *non-custodial wallet*), kerja sama dengan bursa teregulasi terbukti menjadi pintu masuk yang sangat penting bagi penyidik untuk masuk ke dalam jejak transaksi digital pelaku.

4. Pelajaran dari Kasus untuk Regulasi Influencer Keuangan

Kasus Doni Salmanan dan *influencer* sejenisnya memberikan pelajaran yang sangat berharga bagi regulator. Kasus ini menelanjangi bahaya dari fenomena *Financial Influencer* (Finfluencer) yang tidak teregulasi. Banyak masyarakat, terutama pemula, yang menaruh kepercayaan besar pada saran investasi dari para *influencer* tanpa menyadari adanya potensi konflik kepentingan yang besar, seperti skema afiliasi di mana *influencer* diuntungkan dari kerugian pengikutnya.

Pelajaran pertama adalah urgensi untuk menciptakan regulasi yang jelas bagi para *finfluencer*. Regulator seperti OJK dan Bappebti perlu menetapkan aturan main tentang siapa yang boleh memberikan saran keuangan, jenis promosi apa yang diizinkan, dan kewajiban untuk secara transparan mengungkapkan semua bentuk komisi atau konflik kepentingan. Di beberapa negara, individu yang memberikan saran investasi harus memiliki lisensi khusus.

Pelajaran kedua adalah pentingnya literasi keuangan dan digital di masyarakat. Edukasi yang masif perlu terus dilakukan untuk mengajari masyarakat cara membedakan antara saran investasi yang kredibel dengan promosi yang menyesatkan. Masyarakat perlu diajarkan untuk selalu bersikap skeptis, melakukan riset sendiri (*Do Your Own Research* - DYOR), dan memahami bahwa janji keuntungan tinggi yang instan hampir selalu

merupakan pertanda bahaya. Kasus ini menunjukkan bahwa penegakan hukum di hilir harus diimbangi dengan penguatan pertahanan masyarakat di hulu melalui edukasi.

C. Kasus Peretasan dan Pencurian Data yang Melibatkan Kripto

Kasus peretasan dan pencurian data merupakan kejahatan siber murni yang sering kali bersinggungan dengan *cryptocurrency*, baik sebagai target pencurian maupun sebagai alat untuk menjual data curian. Berbeda dengan kasus penipuan yang meninggalkan banyak jejak interaksi sosial, kasus peretasan sering kali lebih sulit diungkap karena pelakunya yang sangat anonim dan jejaknya yang bersifat teknis. Sub-bab ini akan membahas contoh kasus, tantangan identifikasi pelaku, penerapan UU ITE, dan upaya pemulihan asetnya.

1. Contoh Kasus (jika ada data publik)

Di Indonesia, data publik mengenai kasus peretasan yang secara spesifik menargetkan aset kripto individu atau bursa dan berhasil diungkap hingga ke pengadilan masih sangat terbatas. Banyak insiden peretasan yang tidak dilaporkan oleh korban karena malu atau tidak percaya pada penegak hukum, atau diselesaikan secara internal oleh perusahaan untuk menjaga reputasi. Namun, beberapa jenis kasus dapat diangkat sebagai contoh ilustratif berdasarkan laporan media dan pengumuman dari pihak berwenang.

Salah satu contoh adalah kasus *SIM swap fraud*. Dalam modus ini, pelaku menipu operator seluler untuk mentransfer nomor ponsel korban ke kartu SIM baru yang dikuasai pelaku. Dengan menguasai nomor ponsel korban, pelaku kemudian dapat mereset kata sandi berbagai akun online korban, termasuk akun email dan akun bursa kripto, dengan memanfaatkan mekanisme pemulihan akun melalui SMS (OTP). Setelah berhasil mengambil alih akun bursa, pelaku dengan cepat melikuidasi semua aset kripto korban dan mentransfernya ke dompet lain.

Contoh lainnya adalah penyebaran *malware* atau *trojan* yang dirancang khusus untuk mencuri *private key* atau kredensial *crypto wallet*. *Malware* ini bisa disebarkan melalui email *phishing*, tautan di media sosial, atau

perangkat lunak bajakan. Begitu terinstal di perangkat korban, *malware* akan memindai file yang berisi informasi dompet atau memantau *clipboard* untuk mencuri alamat dompet saat korban melakukan transaksi. Kasus-kasus seperti ini, meskipun sering terjadi, jarang sekali pelakunya berhasil diidentifikasi dan ditangkap karena sifatnya yang sangat tersembunyi.

2. Tantangan dalam Mengidentifikasi Pelaku (Atribusi)

Tantangan terbesar dalam menangani kasus peretasan adalah atribusi, yaitu proses mengidentifikasi siapa pelaku di balik sebuah serangan siber. Para peretas profesional sangat mahir dalam menyembunyikan jejak mereka. Mereka menggunakan serangkaian teknik untuk mengaburkan identitas dan lokasi mereka, seperti menggunakan Jaringan Pribadi Virtual (VPN), jaringan anonimitas Tor, atau meretas serangkaian komputer lain (*proxy chain*) untuk melancarkan serangan, sehingga alamat IP asli mereka tidak terekspos.

Dalam kasus pencurian kripto, setelah berhasil mendapatkan aset, pelaku akan segera memindahkannya melalui serangkaian dompet baru dan sering kali menggunakan layanan *mixer* atau *tumbler*. Layanan ini bekerja dengan mencampurkan koin dari berbagai sumber, sehingga sangat sulit untuk melacak hubungan antara koin yang masuk dan koin yang keluar. Penggunaan *privacy coins* seperti Monero juga menjadi pilihan untuk memutuskan jejak transaksi sepenuhnya.

Tantangan-tantangan teknis ini membuat kerja penyidik siber menjadi luar biasa sulit. Tanpa adanya kesalahan operasional dari pihak peretas (misalnya, secara tidak sengaja menggunakan alamat IP asli atau menghubungkan dompet hasil curian dengan akun bursa yang terverifikasi atas nama mereka), kemungkinan untuk mengidentifikasi pelaku menjadi sangat kecil. Inilah sebabnya mengapa tingkat pengungkapan kasus peretasan jauh lebih rendah dibandingkan dengan kasus penipuan.

3. Penerapan Pasal-Pasal dalam UU ITE

Jika pelaku berhasil diidentifikasi, UU ITE menyediakan perangkat hukum yang cukup untuk menjerat mereka. Pasal utama yang akan digunakan adalah Pasal 30 UU ITE tentang Akses Ilegal. Ayat (1) menjerat perbuatan mengakses sistem elektronik milik orang lain tanpa hak. Ayat

(2) menjerat perbuatan mengambil alih kontrol sistem elektronik. Dan Ayat (3) menjerat perbuatan memperoleh informasi elektronik dari sistem tersebut. Dalam kasus *SIM swap* atau peretasan akun bursa, semua ayat ini dapat diterapkan.

Selain itu, Pasal 32 UU ITE tentang Interferensi Data juga sangat relevan. Pasal ini melarang perbuatan mengubah, merusak, atau menghilangkan informasi elektronik. Ketika peretas mengubah kata sandi akun korban atau mentransfer aset kripto keluar dari dompet korban, ia telah melakukan interferensi terhadap data kepemilikan aset digital korban.

Sanksi pidana untuk pelanggaran pasal-pasal ini cukup berat, dengan ancaman hukuman penjara hingga 10 tahun dan denda miliaran rupiah, tergantung pada pasal yang dilanggar. Jika peretasan tersebut menyebabkan kerugian finansial yang signifikan, pasal-pasal ini memberikan dasar yang kuat bagi jaksa untuk menuntut hukuman yang maksimal. Masalahnya bukan pada ketiadaan hukum, melainkan pada kesulitan untuk membawa pelaku ke hadapan hukum.

4. Upaya Pemulihan Aset yang Dicuri

Pemulihan aset (*asset recovery*) dalam kasus peretasan kripto adalah tantangan yang lebih besar lagi. Berbeda dengan sistem perbankan di mana transfer dapat dibatalkan atau dibekukan dalam jangka waktu tertentu, transaksi *cryptocurrency* bersifat *irreversible* (tidak dapat dibatalkan). Sekali sebuah transaksi dikonfirmasi di *blockchain*, tidak ada pihak yang dapat membatalkannya. Ini berarti, jika aset sudah berhasil ditransfer keluar dari akun korban, satu-satunya harapan adalah melacaknya.

Upaya pemulihan biasanya melibatkan kerja sama dengan perusahaan analisis *blockchain* (seperti Chainalysis atau Elliptic) untuk melacak aliran dana curian. Tujuannya adalah untuk melihat apakah dana tersebut pada akhirnya mendarat di sebuah bursa teregulasi. Jika ya, penegak hukum dapat segera menghubungi bursa tersebut dengan bukti-bukti yang ada dan meminta pembekuan akun penerima. Proses ini sangat bergantung pada kecepatan dan kerja sama internasional, karena bursa tersebut bisa berada di yurisdiksi mana pun di dunia.

Namun, jika pelaku berhasil mencairkan dana melalui bursa tidak teregulasi, platform P2P anonim, atau menukarnya dengan *privacy coins*, peluang untuk pemulihan aset menjadi mendekati nol. Realitas yang pahit ini menekankan pentingnya pencegahan dari sisi pengguna. Mengamankan aset kripto dengan *hardware wallet*, menggunakan kata sandi yang kuat dan unik, serta mengaktifkan otentikasi dua faktor (2FA) non-SMS (seperti Google Authenticator) adalah langkah-langkah pertahanan yang jauh lebih efektif daripada berharap pada pemulihan aset setelah peretasan terjadi.

D. Kasus Penggunaan Kripto untuk Transaksi Narkotika

Penggunaan *cryptocurrency* sebagai alat pembayaran di pasar gelap (*dark web*) untuk transaksi narkotika adalah salah satu kasus penggunaan ilegal paling awal dari teknologi ini. Di Indonesia, Badan Narkotika Nasional (BNN) dan Direktorat Tindak Pidana Narkoba Polri telah beberapa kali mengungkap kasus di mana jaringan pengedar menggunakan aset kripto untuk memfasilitasi bisnis haram mereka. Sub-bab ini akan membahas pengungkapan kasus, kolaborasi antar lembaga, dan tantangan pembuktiannya.

1. Pengungkapan Kasus oleh BNN atau Polri

Pengungkapan kasus narkotika yang melibatkan *cryptocurrency* di Indonesia menunjukkan evolusi modus operandi para pengedar. Jaringan narkotika, terutama yang berskala internasional, semakin sadar bahwa transaksi melalui sistem perbankan konvensional sangat mudah dilacak oleh PPATK. Oleh karena itu, mereka beralih ke aset kripto, terutama Bitcoin (BTC) dan Tether (USDT), sebagai medium untuk pembayaran antara bandar, kurir, dan pembeli, serta untuk mencuci keuntungan yang mereka peroleh.

Dalam beberapa kasus yang diungkap oleh BNN, jaringan narkotika internasional mengirimkan narkoba ke Indonesia, dan pembayarannya dilakukan oleh jaringan lokal dengan mentransfer *cryptocurrency* ke alamat dompet yang dikendalikan oleh bandar di luar negeri. Modus ini memungkinkan mereka untuk memindahkan dana dalam jumlah besar lintas batas dengan cepat dan tanpa melalui pengawasan perbankan. Para pelaku lokal biasanya membeli aset kripto dari bursa domestik menggunakan rekening bank atas nama orang lain (rekening nomine) untuk menyamarkan identitas mereka.

Pengungkapan kasus-kasus ini sering kali tidak dimulai dari pelacakan transaksi kripto itu sendiri, melainkan dari metode investigasi konvensional seperti pengintaian, penyadapan, atau penangkapan kurir. Setelah penangkapan terjadi dan perangkat elektronik pelaku (ponsel atau laptop) diperiksa, barulah bukti-bukti penggunaan *cryptocurrency* ditemukan. Dari sinilah penyidik kemudian mulai menelusuri jejak digital transaksi narkotika tersebut.

2. Kolaborasi Antar Lembaga dalam Penindakan

Keberhasilan pengungkapan kasus narkotika berbasis kripto sangat bergantung pada kolaborasi yang erat antar lembaga. Tidak ada satu lembaga pun yang memiliki semua keahlian yang dibutuhkan. BNN dan Polri memiliki keahlian dalam investigasi jaringan narkotika, tetapi mungkin tidak memiliki kapasitas mendalam dalam analisis *blockchain*. Di sinilah peran lembaga lain menjadi krusial.

Kolaborasi utama terjalin dengan **PPATK**. PPATK membantu menganalisis transaksi keuangan yang terkait dengan pembelian aset kripto oleh jaringan tersebut. Jika sebuah rekening bank menunjukkan aktivitas mencurigakan terkait pembelian kripto dalam jumlah besar, PPATK dapat melaporkannya kepada BNN atau Polri sebagai petunjuk awal. Sebaliknya, setelah BNN menangkap pelaku, mereka dapat meminta bantuan PPATK dan Dittipidsiber Bareskrim Polri untuk melakukan analisis *on-chain* terhadap alamat-alamat dompet yang ditemukan.

Kerja sama juga terjalin dengan bursa aset kripto yang terdaftar di Bappebti. Sebagai pihak pelapor, bursa memiliki kewajiban untuk melaporkan transaksi mencurigakan. Selain itu, ketika penyidik datang dengan surat perintah yang sah, bursa wajib memberikan data identitas (KYC) dan riwayat transaksi dari akun yang diduga terlibat. Kolaborasi segitiga antara lembaga penegak hukum (BNN/Polri), lembaga intelijen keuangan (PPATK), dan sektor swasta (bursa kripto) menjadi formula kunci dalam membongkar jaringan ini.

3. Pembuktian Transaksi Kripto di Pengadilan

Membuktikan bahwa sebuah transaksi kripto terkait dengan kejahatan narkotika di pengadilan adalah sebuah tantangan. Jaksa tidak cukup hanya

menunjukkan adanya transfer Bitcoin dari A ke B. Jaksa harus mampu membangun sebuah narasi yang meyakinkan hakim bahwa transfer tersebut merupakan pembayaran untuk narkotika, bukan untuk tujuan lain yang sah. Hal ini memerlukan kombinasi bukti digital dan bukti konvensional.

Bukti digital yang diajukan biasanya berupa data dari bursa yang menunjukkan pembelian kripto oleh terdakwa, data dari *blockchain explorer* yang menunjukkan transfer ke alamat dompet bandar, dan data forensik dari ponsel terdakwa. Data forensik ini bisa menjadi kunci, misalnya berupa percakapan di aplikasi pesan terenkripsi di mana terdakwa dan bandar menyepakati jumlah narkotika dan alamat dompet untuk pembayaran. Kombinasi antara bukti percakapan dan bukti transaksi *blockchain* yang cocok (jumlah dan waktunya) akan menjadi *qarīnah* (indikasi) yang sangat kuat.

Selain bukti digital, bukti konvensional tetap vital. Kesaksian dari kurir yang tertangkap, barang bukti narkotika yang disita, dan hasil pengintaian yang menunjukkan pertemuan antara para pelaku semuanya akan dirangkai bersama bukti digital untuk membentuk sebuah gambaran utuh di hadapan hakim. Keberhasilan jaksa dalam "mendidik" hakim mengenai cara kerja transaksi kripto dan menghubungkannya dengan bukti-bukti lain menjadi faktor penentu dalam proses pembuktian.

4. Analisis Efektivitas Penegakan Hukum

Efektivitas penegakan hukum terhadap kasus narkotika berbasis kripto di Indonesia menunjukkan gambaran yang beragam. Di satu sisi, keberhasilan dalam mengungkap beberapa kasus besar menunjukkan bahwa aparat penegak hukum Indonesia tidak buta terhadap modus operandi baru ini. Kemampuan untuk menjalin kerja sama antar lembaga dan memanfaatkan data dari bursa teregulasi adalah sebuah kekuatan yang signifikan.

Di sisi lain, harus diakui bahwa kasus-kasus yang terungkap kemungkinan besar hanyalah puncak dari gunung es. Jaringan yang lebih canggih mungkin sudah beralih menggunakan metode yang lebih sulit dilacak, seperti transaksi P2P secara langsung, penggunaan *mixer*,

atau *privacy coins*. Kapasitas teknis penyidik untuk melakukan analisis *blockchain* yang mendalam dan melintasi berbagai yurisdiksi masih perlu terus ditingkatkan secara masif.

Efektivitas penegakan hukum juga diukur dari kemampuannya untuk menjerat pelaku dengan pasal pencucian uang (TPPU), tidak hanya dengan UU Narkotika. Dengan menjerat bandar dengan TPPU, negara dapat merampas seluruh keuntungan yang mereka peroleh, memiskinkan mereka, dan melumpuhkan kapasitas operasional jaringan mereka. Penindakan yang hanya fokus pada kurir atau pengedar kecil tanpa menyentuh aliran dananya tidak akan pernah efektif dalam jangka panjang. Oleh karena itu, integrasi penyidikan narkotika dengan penyidikan TPPU adalah kunci efektivitas di masa depan.

E. Analisis Komparatif Putusan Pengadilan

Setelah menganalisis berbagai jenis kasus, langkah terakhir dalam bab ini adalah melakukan analisis komparatif terhadap putusan-putusan pengadilan yang telah berkekuatan hukum tetap. Dengan membandingkan pertimbangan hukum hakim (*ratio decidendi*) dalam kasus-kasus yang serupa, kita dapat menilai tingkat konsistensi penerapan hukum dan bagaimana hakim berperan dalam menggali nilai keadilan. Analisis ini penting untuk melihat arah perkembangan yurisprudensi kejahatan ekonomi digital di Indonesia.

1. Perbandingan Pertimbangan Hakim dalam Kasus Serupa

Dengan membandingkan putusan dalam kasus-kasus penipuan investasi (misalnya, antara kasus robot trading yang berbeda atau antara kasus robot trading dengan kasus *binary option*), kita dapat melihat bagaimana hakim menafsirkan unsur-unsur delik. Misalnya, bagaimana hakim mendefinisikan "tipu muslihat" atau "rangkaian kebohongan" dalam konteks promosi digital? Apakah hakim secara konsisten melihat model bisnis afiliasi sebagai bentuk skema piramida yang dilarang?

Dalam beberapa kasus, mungkin ditemukan perbedaan penekanan. Satu majelis hakim mungkin lebih fokus pada aspek penipuan konvensional (KUHP), sementara majelis lain mungkin lebih menekankan pada pelanggaran

UU Perdagangan atau UU ITE. Perbandingan ini dapat mengungkapkan pemahaman yang berbeda di antara para hakim mengenai instrumen hukum mana yang paling tepat untuk kejahatan digital.

Perbandingan yang paling menarik sering kali muncul dalam putusan terkait TPPU, khususnya mengenai perampasan aset. Membandingkan putusan kasus Doni Salmanan (di mana aset akhirnya dirampas untuk negara) dengan putusan kasus Indra Kenz (di mana aset diputuskan untuk dikembalikan kepada para korban) menunjukkan adanya diskresi dan bahkan perbedaan pandangan yang signifikan di antara majelis hakim dalam menafsirkan keadilan bagi korban kejahatan massal.

2. Konsistensi Penerapan Hukum

Konsistensi dalam penerapan hukum adalah salah satu pilar utama dari kepastian hukum. Analisis komparatif memungkinkan kita untuk menilai apakah hukum diterapkan secara konsisten pada kasus-kasus yang memiliki fakta hukum yang serupa. Inkonsistensi dapat menimbulkan ketidakpastian dan rasa ketidakadilan. Misalnya, jika dua orang afiliator *binary option* dengan peran dan keuntungan yang serupa mendapatkan vonis yang sangat jauh berbeda (satu dihukum berat, satu dihukum ringan), hal ini dapat mencederai kepercayaan publik pada sistem peradilan.

Analisis ini juga dapat menyoroti apakah ada "tren" dalam pemidanaan. Apakah hukuman untuk kejahatan siber cenderung semakin berat seiring waktu, seiring dengan meningkatnya kesadaran akan bahayanya? Apakah pengadilan semakin sering menggunakan UU TPPU sebagai delik pamungkas? Mengidentifikasi tren ini penting untuk memprediksi arah penegakan hukum di masa depan.

Inkonsistensi tidak selalu berarti buruk jika didasarkan pada pertimbangan yang matang mengenai fakta-fakta spesifik dari setiap kasus. Namun, jika inkonsistensi tersebut tampak acak atau tidak memiliki dasar pertimbangan yang jelas, maka ini menjadi sinyal bagi Mahkamah Agung atau lembaga pelatihan hakim untuk melakukan evaluasi dan menyelenggarakan pelatihan guna menyeragamkan persepsi dalam penanganan perkara kejahatan siber.

3. Peran Hakim dalam Menggali Nilai Keadilan

Hakim di Indonesia tidak hanya bertindak sebagai "corong undang-undang" (positivisme legalistik), tetapi juga memiliki kewajiban untuk menggali, mengikuti, dan memahami nilai-nilai hukum dan rasa keadilan yang hidup dalam masyarakat (hukum progresif). Dalam kasus kejahatan digital yang sering kali belum diatur secara sempurna oleh undang-undang, peran hakim sebagai penemu hukum (*rechtsvinding*) menjadi sangat vital.

Analisis putusan dapat menunjukkan sejauh mana hakim berani melakukan penafsiran hukum yang progresif untuk mencapai keadilan materiil. Misalnya, ketika hakim menafsirkan "barang" dalam KUHP untuk mencakup aset kripto yang tidak berwujud, atau ketika hakim memutuskan bahwa *binary option* adalah perjudian meskipun belum ada undang-undang yang secara eksplisit mengaturnya, di situlah hakim sedang menjalankan peran sebagai penemu hukum.

Perdebatan mengenai status aset rampasan (dikembalikan ke korban atau dirampas untuk negara) adalah arena utama di mana hakim menggali nilai keadilan. Hakim yang memutuskan pengembalian aset ke korban sedang memprioritaskan keadilan restoratif bagi korban. Sementara hakim yang memutuskan perampasan untuk negara mungkin memprioritaskan efek jera dan kepastian hukum (karena kesulitan teknis dalam distribusi). Menganalisis argumen di balik pilihan-pilihan ini memberikan wawasan mendalam tentang bagaimana keadilan dinegosiasikan dalam ruang sidang.

4. Implikasi Putusan terhadap Perkembangan Yurisprudensi

Setiap putusan pengadilan, terutama yang telah mencapai tingkat kasasi atau peninjauan kembali di Mahkamah Agung, berpotensi menjadi yurisprudensi. Yurisprudensi adalah putusan hakim terdahulu yang diikuti oleh hakim-hakim lain dalam perkara serupa, dan berfungsi sebagai sumber hukum yang penting di negara-negara dengan sistem hukum campuran seperti Indonesia. Putusan-putusan dalam kasus kejahatan kripto pertama di Indonesia ini akan menjadi fondasi bagi yurisprudensi di masa depan.

Putusan yang mengkualifikasikan *binary option* sebagai perjudian, misalnya, akan menjadi acuan penting bagi kasus-kasus serupa berikutnya. Putusan yang berhasil membuktikan pencucian uang melalui *cryptocurrency* akan memberikan cetak biru bagi jaksa dan hakim lain. Sebaliknya, putusan yang membebaskan pelaku karena kelemahan pembuktian digital juga akan menjadi pelajaran penting, menyoroti area di mana undang-undang atau kapasitas teknis penegak hukum perlu diperkuat.

Analisis terhadap putusan-putusan ini tidak hanya penting bagi akademisi, tetapi juga bagi para praktisi hukum dan legislator. Bagi praktisi, ia memberikan panduan tentang bagaimana membangun argumen dan menyajikan bukti dalam kasus kejahatan siber. Bagi legislator, ia menunjukkan pasal-pasal mana dalam undang-undang yang sudah efektif dan mana yang memerlukan amandemen atau peraturan pelaksana yang lebih jelas. Dengan demikian, putusan-putusan pengadilan dalam kasus-kasus awal ini memainkan peran sentral dalam membentuk evolusi hukum pidana ekonomi digital di Indonesia.

Analisis Mendalam Konsep Kunci Bab 8: Analisis Yuridis Empiris Melalui Studi Kasus

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk membumikan seluruh diskusi hukum ke dalam realitas empiris. Tujuannya bukan lagi membahas "apa kata undang-undang" (analisis normatif), melainkan "bagaimana undang-undang itu digunakan di pengadilan" (analisis yuridis empiris). Bab ini berfungsi untuk:

1. Menguji Efektivitas Hukum: Mengevaluasi sejauh mana "jaring" hukum berlapis yang dijelaskan di Bab 6 benar-benar efektif dalam menjerat pelaku di dunia nyata.
2. Menganalisis Strategi Penegak Hukum: Membedah bagaimana jaksa membangun dakwaan mereka dengan mengombinasikan berbagai pasal dari undang-undang yang berbeda.
3. Mempelajari Pertimbangan Hakim: Mengkaji logika dan pertimbangan hukum (*ratio decidendi*) yang digunakan oleh hakim dalam memutus perkara, termasuk bagaimana mereka menafsirkan unsur-unsur delik.

4. Mengidentifikasi Tantangan Praktis: Menyoroti kesulitan-kesulitan nyata yang dihadapi di lapangan, seperti pembuktian, pelacakan aset, dan identifikasi pelaku.

Ini adalah "uji lapangan" dari semua teori hukum positif yang telah dibahas.

Elemen-Elemen Kunci dalam Analisis Studi Kasus:

1. Kronologi & Modus Operandi: Rekonstruksi peristiwa berdasarkan fakta-fakta yang terungkap di persidangan.
2. Dakwaan Jaksa: Identifikasi pasal-pasal yang digunakan untuk menuntut pelaku.
3. Putusan & Pertimbangan Hakim: Analisis vonis (pidana penjara, denda, perampasan aset) dan alasan hukum di baliknya.
4. Pelajaran yang Dipetik (*Lessons Learned*): Sintesis dari kekuatan, kelemahan, dan implikasi kasus tersebut bagi penegakan hukum di masa depan.

Analisis Komparatif: Penerapan Hukum pada Berbagai Jenis Kasus

Tabel berikut membedah bagaimana kerangka hukum positif diterapkan secara berbeda pada berbagai jenis studi kasus kejahatan kripto di Indonesia.

Aspek Analisis	Kasus Penipuan Investasi (*Robot Trading*)	Kasus Pencucian Uang (*Influencer*)	Kasus Peretasan (*Hacking*)	Kasus Transaksi Narkotika
Contoh Kasus	Fahrenheit, Net89	Doni Salmanan (Binary Option, terkait Kripto)	Kasus peretasan bursa (jika ada data publik)	Pengungkapan jaringan oleh BNN/Polri
Fokus Utama Penegakan Hukum	Membuktikan unsur penipuan dan perdagangan ilegal.	Membuktikan penerimaan dana hasil kejahatan dan penyebaran berita bohong.	Membuktikan akses ilegal dan pencurian data/aset.	Membuktikan transaksi narkotika dan penggunaan kripto sebagai metode pembayaran.
Kombinasi UU yang Digunakan (Dakwaan Berlapis)	KUHP (Pasal 378) + UU Perdagangan + UU TPPU.	UU ITE (Pasal 28 & 45A) + UU TPPU (Pasal 3).	UU ITE (Pasal 30 & 32) + KUHP (Pasal 362 - Pencurian).	UU Narkotika + UU TPPU.
Tantangan Pembuktian Utama	Membuktikan "niat jahat" (*mens rea*) dan membedakannya dari risiko bisnis biasa. Menghitung kerugian korban yang masif.	Menunjukkan bahwa *influencer* mengetahui atau seharusnya menduga bahwa dana yang diterimanya berasal dari tindak pidana.	Atribusi Pelaku: Mengidentifikasi hacker yang sering kali anonim dan beroperasi dari luar negeri.	Menghubungkan alamat dompet kripto yang anonim dengan terdakwa secara meyakinkan.
Peran Kunci Lembaga Lain	BAPPEBTI/OJK sebagai pemberi keterangan ahli tentang legalitas investasi.	PPATK untuk melacak aliran dana dari korban ke *influencer* dan aset-aset yang dibeli.	Ahli Forensik Digital untuk menganalisis jejak peretasan. Interpol untuk kerja sama internasional.	PPATK untuk analisis transaksi. BNN sebagai penyelidik utama kejahatan asal.

Aspek Analisis	Kasus Penipuan Investasi (*Robot Trading*)	Kasus Pencucian Uang (*Influencer*)	Kasus Peretasan (*Hacking*)	Kasus Transaksi Narkotika
Pelajaran Penting (*Lessons Learned*)	Pentingnya regulasi yang ketat untuk robot trading dan skema serupa. Efektivitas dakwaan berlapis.	Bahaya *finfluencer* yang tidak teregulasi. Pentingnya literasi keuangan digital bagi masyarakat.	Mendesaknya peningkatan kapasitas forensik digital dan kerja sama internasional.	Kripto telah menjadi metode pembayaran standar bagi jaringan kejahatan terorganisir.

Kontribusi Konsep Studi Kasus dalam Bab 8:

Konsep ini adalah jembatan antara hukum dalam teks (*law in books*) dan hukum dalam aksi (*law in action*).

1. Memberikan Bukti Empiris: Bab ini menyajikan bukti nyata bahwa undang-undang yang dibahas di Bab 6 bukan hanya macan kertas, tetapi benar-benar digunakan untuk menghukum pelaku.
2. Menunjukkan Pola Penegakan Hukum: Analisis berbagai kasus memungkinkan pembaca untuk melihat pola: bagaimana aparat penegak hukum cenderung mengombinasikan UU ITE dan UU TPPU sebagai "pukulan satu-dua" yang efektif.
3. Menjadi Dasar untuk Analisis Fikih Lanjutan (Bab 9): Kasus-kasus konkret inilah (Fahrenheit, Doni Salmanan, dll.) yang akan menjadi "objek" analisis dalam Bab 9. Bab 9 akan bertanya, "Bagaimana fikih jinayah memandang kasus Fahrenheit dari sudut pandang *gharar* dan *tadlis*?"
4. Menghasilkan Rekomendasi yang Membumi: Kelemahan-kelemahan praktis yang terungkap dalam bab ini (misalnya, kesulitan pemulihan aset, lamanya proses) akan menjadi dasar bagi rekomendasi kebijakan yang konkret dan realistis di bab-bab penutup.

Secara ringkas, Bab 8 mengubah buku ini dari sekadar risalah teoretis menjadi sebuah analisis yang relevan dengan kenyataan. Ia menunjukkan kepada pembaca, melalui contoh-contoh nyata, bagaimana negara berupaya (dan terkadang kesulitan) untuk menegakkan hukum di perbatasan liar ekonomi digital.

BAB 9

Pandangan dari Perspektif Hukum Pidana Islam

Setelah pada Bab 8 kita membedah berbagai studi kasus dari kacamata hukum positif, Bab 9 ini akan kembali pada kerangka hukum pidana Islam untuk melakukan analisis tandingan. Tujuan bab ini bukanlah untuk menghakimi putusan pengadilan yang sudah ada, melainkan untuk memberikan perspektif fikih yang kaya terhadap fakta-fakta hukum yang sama. Dengan melakukan *takhyīf fiqhī* (kualifikasi fikih) terhadap kasus-kasus nyata, kita dapat melihat secara konkret bagaimana konsep-konsep seperti *gharar*, *tadlīs*, *sariqah*, dan *ta'zīr* dapat diaplikasikan pada modus operandi kejahatan abad ke-21 (Al-Qaradawi, 1999). *Research gap* yang diisi adalah kurangnya aplikasi langsung dari teori fikih jinayah pada data empiris kasus-kasus kejahatan kripto yang telah diputus oleh pengadilan di Indonesia. Pertanyaan penelitian utama yang akan dijawab adalah: Bagaimana kasus-kasus penipuan investasi, pencucian uang, peretasan, dan transaksi narkotika yang melibatkan *cryptocurrency* di Indonesia dapat dianalisis dan dikualifikasikan menurut hukum pidana Islam, dan rekomendasi sanksi serta kebijakan apa yang dapat ditarik dari analisis tersebut?

A. Pandangan Robot Trading sebagai Penipuan (Gharar dan Tadlis)

Kasus penipuan investasi berkedok robot trading seperti Fahrenheit dan Net89, yang menjanjikan keuntungan pasti dan tidak realistis, merupakan contoh sempurna dari praktik yang dilarang keras dalam fikih muamalah dan jinayah. Sub-bab ini akan menganalisis kasus tersebut dengan mengidentifikasi unsur *gharar* dan *tadlīs* yang terkandung di dalamnya, mengkualifikasikannya sebagai *jarīmah ta'zīr*, dan merekomendasikan sanksi yang sesuai dengan prinsip keadilan Islam (Ibn Taymiyyah, 1987).

1. Identifikasi Unsur Ketidakpastian (Gharar) yang Dilarang

Gharar, atau ketidakpastian yang berlebihan, merupakan elemen sentral yang membatalkan keabsahan akad dalam hukum muamalah Islam (Al-Zuhaili, 2003). Dalam kasus robot trading, unsur *gharar* sangat kental dan berlapis. Pertama, terdapat *gharar* pada objek akad itu sendiri. Para investor tidak pernah benar-benar tahu bagaimana "robot" tersebut bekerja; algoritmanya adalah sebuah "kotak hitam" (*black box*), yang

mana ketidakjelasan mekanisme ini merupakan bentuk *gharar fahish* (ketidakpastian yang parah) (Saeed, 2016). Mereka menyerahkan uang mereka pada mekanisme yang tidak jelas dan tidak dapat diverifikasi, yang secara langsung bertentangan dengan prinsip transparansi dalam transaksi Islam.

Kedua, janji keuntungan yang pasti dan tetap (misalnya 1% per hari) dari aktivitas trading yang secara inheren tidak pasti adalah bentuk *gharar* yang paling fatal. Dalam Islam, setiap investasi yang melibatkan modal dan usaha (*muḍārabah* atau *musyārakah*) harus didasarkan pada prinsip bagi hasil dan risiko (*al-ghunm bi al-ghurm*), di mana keuntungan tidak dapat dijamin di muka (Chapra, 2000). Menjamin keuntungan secara mutlak adalah sebuah kebohongan dan membatalkan keabsahan akad investasi tersebut, mengubahnya menjadi akad pinjaman yang mensyaratkan tambahan (*qardh bi ziyadah*), yang merupakan salah satu bentuk riba.

Ketiga, penggunaan skema Ponzi, di mana keuntungan investor lama dibayar dari uang investor baru, adalah puncak dari *gharar* dan penipuan. Para investor mengira keuntungan mereka berasal dari hasil trading yang brilian, padahal sesungguhnya berasal dari dana orang lain yang direkrut kemudian (Putusan MA No. 862 K/Pid.Sus/2023). Ketidakjelasan sumber keuntungan ini menjadikan seluruh skema tersebut haram dan batil dari perspektif fikih muamalah, karena keuntungan tidak lahir dari aktivitas ekonomi riil yang produktif.

2. Pembuktian Unsur Penipuan (Tadlis) dalam Pemasaran

Tadlīs adalah tindakan menipu dengan sengaja menyembunyikan cacat atau menampilkan informasi palsu untuk menarik pembeli atau investor, sebuah praktik yang dikutuk dalam banyak hadis Nabi (Ibn Taymiyyah, 1987). Praktik pemasaran yang dilakukan oleh para pelaku dan afiliator robot trading adalah contoh buku teks dari *tadlīs*. Mereka secara aktif dan sistematis menyebarkan informasi bohong untuk membangun citra kesuksesan dan menutupi sifat asli dari skema Ponzi yang mereka jalankan.

Unsur *tadlīs* terbukti dari beberapa hal. Pertama, pameran kemewahan (*flexing*) yang dilakukan oleh para afiliator. Mereka menampilkan mobil sport, jam tangan mahal, dan liburan mewah seolah-olah itu semua adalah

hasil dari kehebatan robot trading (Laporan Media, Kompas, 2022). Padahal, kekayaan tersebut berasal dari komisi perekrutan dan dana para investor itu sendiri. Ini adalah penipuan visual yang dirancang untuk membangkitkan keserakahan (*ṭama'*) dan mematikan rasionalitas calon korban.

Kedua, penggunaan testimoni palsu dan klaim-klaim teknis yang tidak berdasar. Para pelaku sering kali mengklaim bahwa teknologi mereka didukung oleh AI tercanggih atau dikelola oleh tim trader profesional kelas dunia, tanpa pernah memberikan bukti yang dapat diverifikasi (Putusan PN Jakarta Barat No. 711/Pid.Sus/2022). Mereka menyembunyikan fakta bahwa model bisnis mereka adalah skema piramida. Perpaduan antara *gharar* (ketidakpastian dalam akad) dan *tadlīs* (penipuan dalam pemasaran) ini secara jelas mengkategorikan perbuatan mereka sebagai tindakan memakan harta orang lain dengan cara yang batil (*aklu amwāl al-nās bi al-bāṭil*), sebagaimana dilarang dalam QS. An-Nisa: 29.

3. Kualifikasi sebagai Jarimah Ta'zir

Dari perspektif hukum pidana Islam, perbuatan yang mengandung unsur *gharar* dan *tadlīs* yang merugikan banyak orang ini tidak termasuk dalam kategori *hudūd* atau *qiṣāṣ*. Oleh karena itu, ia secara otomatis masuk ke dalam kategori *jarīmah ta'zīr*, yaitu tindak pidana yang jenis dan sanksinya ditentukan oleh penguasa (*ulil amri*) demi mewujudkan kemaslahatan umum (Audah, 2007). Kualifikasi ini memberikan landasan syar'i bagi negara untuk menindak para pelaku.

Perbuatan para pelaku skema robot trading ini telah melanggar beberapa prinsip fundamental syariah sekaligus. Mereka melanggar larangan memakan harta secara batil (QS. An-Nisa: 29), larangan penipuan, dan menyebabkan kerusakan finansial yang masif di tengah masyarakat. Dengan demikian, negara tidak hanya berhak, tetapi juga berkewajiban untuk mengkriminalisasi perbuatan ini dan mengadili para pelakunya sebagai bentuk perlindungan terhadap harta masyarakat (*ḥifẓ al-māl*), yang merupakan salah satu dari lima tujuan utama syariah (Auda, 2008).

Undang-undang positif yang digunakan oleh jaksa (KUHP, UU Perdagangan, UU ITE) dapat dipandang sebagai manifestasi dari legislasi *ta'zīr* yang dibuat oleh negara Indonesia. Ketika hakim menghukum para

pelaku berdasarkan undang-undang tersebut, pada hakikatnya ia sedang menjalankan fungsi penegakan *jarīmah ta'zīr* yang telah ditetapkan oleh otoritas yang sah, yang sepenuhnya sejalan dengan prinsip *siyāsah syar'iyyah* (Hallaq, 2009).

4. Rekomendasi Sanksi Ta'zir yang Sesuai (Ganti Rugi, Penjara)

Dalam menentukan sanksi *ta'zīr* yang sesuai, hakim dalam perspektif Islam harus mempertimbangkan beberapa tujuan: efek jera (*zawājir*), pemulihan hak korban (*restitusi*), dan perbaikan (*iṣlāḥ*) (Kamali, 2000). Untuk kasus penipuan massal seperti ini, sanksi yang direkomendasikan harus bersifat komprehensif. Prioritas pertama dan utama adalah pengembalian kerugian korban (*ḍamān*). Seluruh aset yang berhasil disita dari para pelaku harus diprioritaskan untuk dikembalikan kepada para korban secara proporsional. Ini adalah implementasi dari keadilan restoratif dan kewajiban mengembalikan harta yang diambil secara tidak sah.

Kedua, untuk memberikan efek jera, sanksi penjara (*al-ḥabs*) dalam jangka waktu yang lama sangat diperlukan, terutama bagi para otak intelektual dan petinggi skema tersebut. Durasi hukuman harus sepadan dengan skala kerugian dan jumlah korban yang ditimbulkan (Audah, 2007). Hukuman ini berfungsi sebagai balasan atas perbuatan mereka dan sebagai pelajaran bagi masyarakat agar tidak mencoba melakukan kejahatan serupa.

Ketiga, sanksi tambahan seperti publikasi putusan dan identitas pelaku (*tasyhīr*) sangat relevan untuk mempermalukan pelaku dan memberikan peringatan yang lebih luas kepada publik (Al-Mawardi, 1996). Selain itu, sanksi berupa larangan seumur hidup untuk beraktivitas di sektor jasa keuangan juga dapat diterapkan untuk mencegah pelaku mengulangi perbuatannya di masa depan. Kombinasi dari sanksi pemulihan, sanksi badan, dan sanksi sosial ini diharapkan dapat mewujudkan keadilan yang lebih utuh.

B. Pandangan Pencucian Uang sebagai I'anah 'ala al-Ma'siyah

Kasus pencucian uang yang dilakukan oleh *influencer* seperti Doni Salmanan, yang menikmati hasil dari mempromosikan platform investasi ilegal, memberikan contoh nyata tentang bagaimana seseorang dapat dimintai pertanggungjawaban karena membantu keberlangsungan sebuah kejahatan. Sub-bab ini akan menganalisis perbuatan tersebut dari perspektif fikih sebagai bentuk *i'ānah 'alā al-ma'ṣiyah* (bantuan terhadap kemaksiatan), membahas tanggung jawab pidananya, dan kewajiban terkait harta yang diperolehnya (Al-Qaradawi, 1999).

1. Mengkategorikan Perbuatan sebagai Bantuan terhadap Kejahatan

Perbuatan Doni Salmanan sebagai afiliator platform Quotex dapat dikategorikan sebagai *i'ānah 'alā al-ma'ṣiyah*. Kejahatan atau "kemaksiatan" utamanya adalah platform *binary option* itu sendiri, yang oleh para ulama kontemporer dikategorikan mengandung unsur perjudian (*maysir*) dan penipuan (*tadlīs*) (Majelis Ulama Indonesia, 2021). Dengan menjadi afiliator, ia tidak hanya berpartisipasi, tetapi secara aktif mengajak, mempromosikan, dan memfasilitasi orang lain untuk terjerumus ke dalam praktik haram tersebut. Ia adalah jembatan yang menghubungkan korban dengan platform kejahatan.

Prinsip dalam hukum Islam sangat jelas: "*wa lā ta'āwanū 'ala al-ithmi wa al-'udwān*" (dan jangan tolong-menolong dalam berbuat dosa dan pelanggaran) (QS. Al-Ma'idah: 2). Peran seorang afiliator adalah bentuk "tolong-menolong dalam dosa" yang paling nyata. Ia menyediakan sarana (informasi dan tautan pendaftaran) dan motivasi (iming-iming keuntungan) yang memungkinkan kejahatan tersebut berkembang pesat (Putusan MA No. 862 K/Pid.Sus/2023). Tanpa para afiliator, platform seperti Quotex tidak akan mampu menjangkau korban dalam jumlah massal.

Oleh karena itu, meskipun ia bukan pemilik atau operator platform, perbuatannya sebagai "corong pemasaran" kejahatan membuatnya turut bertanggung jawab atas kerugian yang diderita oleh para pengikutnya. Ia tidak bisa berlindung di balik argumen bahwa ia hanya seorang promotor. Dalam fikih, orang yang menunjukkan jalan menuju kejahatan

dan mengambil keuntungan darinya dapat dimintai pertanggungjawaban pidana sebagai pelaku penyerta (*syarīk*) atau pembantu (*mu'īn*) (Audah, 2007).

2. Tanggung Jawab Pidana Pelaku Pencucian Uang

Setelah mendapatkan keuntungan dari perbuatan haramnya (menjadi afiliator), tindakan selanjutnya yaitu membelanjakan, menyembunyikan, dan mengubah bentuk harta tersebut adalah inti dari pencucian uang. Dari perspektif Islam, ini adalah kejahatan berlapis. Pertama, ia menikmati harta yang diperoleh dari sumber yang haram, yang itu sendiri sudah merupakan dosa (Al-Qaradawi, 1999). Kedua, dengan melakukan pencucian uang, ia berusaha menyamarkan status haram dari harta tersebut dan membuatnya seolah-olah halal, yang merupakan bentuk penipuan lebih lanjut.

Tanggung jawab pidananya sebagai pelaku pencucian uang dapat dikategorikan sebagai *jarīmah ta'zīr*. Negara berhak menetapkan sanksi bagi siapa saja yang terbukti menyembunyikan atau menyamarkan harta hasil kejahatan (Hallaq, 2009). Tindakan ini dikriminalisasi karena ia merusak integritas sistem ekonomi dan mempersulit upaya penegak hukum untuk melacak kejahatan asalnya. UU TPPU dalam hukum positif Indonesia adalah cerminan dari kebijakan *ta'zīr* yang sejalan dengan semangat syariah untuk memberantas segala bentuk fasilitasi kejahatan.

Hukuman *ta'zīr* yang dijatuhkan haruslah berat, karena pencucian uang adalah kejahatan yang menjadi "pelumas" bagi kejahatan lainnya. Dengan menghukum berat para pelaku pencucian uang, negara mengirimkan pesan bahwa tidak ada tempat yang aman untuk menyembunyikan hasil kejahatan (Kamali, 2000). Ini akan memberikan efek jera tidak hanya bagi pelaku pencucian uang itu sendiri, tetapi juga bagi para pelaku kejahatan primer.

3. Kewajiban Mengembalikan Harta kepada yang Berhak

Prinsip utama dalam hukum Islam mengenai harta haram adalah kewajiban untuk mengembalikannya (*ḍamān*). Harta yang diperoleh Doni Salmanan dari komisi kerugian para pengikutnya bukanlah haknya. Itu adalah harta milik para korban yang diambil secara batil melalui tipu daya (Ibn Taymiyyah, 1987). Oleh karena itu, kewajiban pertama dan utama bagi

pelaku (atau bagi negara setelah menyita hartanya) adalah mengembalikan harta tersebut kepada para korban yang dapat diidentifikasi.

Putusan pengadilan yang pada akhirnya memutuskan aset dirampas untuk negara, dari perspektif fikih, dapat diperdebatkan. Prioritas tertinggi seharusnya adalah restitusi kepada korban (Al-Zuhaili, 2003). Argumen bahwa sulit untuk mengidentifikasi korban mungkin benar secara teknis, tetapi tidak boleh mengalahkan prinsip keadilan restoratif. Seharusnya, negara mengerahkan upaya maksimal untuk membuat mekanisme pendataan dan verifikasi korban guna memungkinkan pengembalian aset, sejalan dengan semangat *iṣlāḥ* (perbaikan).

Jika setelah upaya maksimal dilakukan masih ada korban yang tidak dapat diidentifikasi atau sisa aset yang tidak terdistribusi, barulah sisa harta tersebut dapat dirampas untuk negara (Al-Qaradawi, 1999). Namun, menempatkan perampasan untuk negara sebagai pilihan pertama, sementara para korban yang menderita kerugian langsung tidak mendapatkan apa-apa, kurang selaras dengan semangat *ḥifẓ al-māl* dan keadilan restoratif yang menjadi inti dari *Maqāshid al-Sharī'ah* (Auda, 2008).

4. Konsep Perampasan Harta untuk Baitul Mal

Dalam skenario di mana pengembalian kepada korban tidak memungkinkan, konsep perampasan harta untuk *bayt al-māl* (kas negara) menjadi relevan. Harta tersebut tidak boleh dibiarkan dinikmati oleh pelaku atau keluarganya (Audah, 2007). Negara mengambil alih harta tersebut untuk dimanfaatkan bagi kemaslahatan umum (*maṣlaḥah 'āmah*), seperti membiayai program sosial, pendidikan, atau kesehatan.

Tindakan merampas aset untuk negara dalam putusan kasus Doni Salmanan, jika dilihat dari sudut pandang ini, memiliki landasan fikihnya sebagai alternatif terakhir. Ini jauh lebih baik daripada membiarkan aset tersebut kembali ke tangan pelaku, seperti yang sempat diputuskan di tingkat banding (Putusan PN Bale Bandung No. 683/Pid.Sus/2022). Perampasan untuk negara memastikan bahwa "kejahatan tidak menghasilkan keuntungan". Dana yang masuk ke kas negara ini kemudian dapat digunakan untuk membiayai program-program publik, termasuk program edukasi literasi keuangan untuk mencegah jatuhnya korban-korban baru di masa depan.

Dengan demikian, meskipun prioritas utama adalah pengembalian kepada korban, perampasan untuk negara adalah pilihan sekunder yang dapat dibenarkan secara syar'i. Hal ini sejalan dengan tujuan untuk membersihkan sistem ekonomi dari harta haram dan mengalihkannya untuk tujuan yang produktif dan bermanfaat bagi masyarakat luas (Chapra, 2000).

C. Pandangan Peretasan sebagai Sariqah Ta'ziriyah

Peretasan yang bertujuan mencuri aset kripto dari dompet digital atau akun bursa adalah bentuk modern dari pencurian. Namun, karena sifatnya yang non-fisik dan menggunakan metode canggih, kualifikasinya dalam hukum pidana Islam memerlukan analisis yang cermat. Sub-bab ini akan berargumen mengapa peretasan lebih tepat dikategorikan sebagai *sariqah ta'zīriyah* (pencurian *ta'zīr*) daripada *sariqah hudūd*, serta membahas bagaimana sanksi dan pemulihan asetnya diatur (Kamali, 2000).

1. Argumentasi Mengapa Tidak Termasuk Hudud

Penerapan sanksi *hadd* (potong tangan) untuk pencurian (*sariqah*) mensyaratkan terpenuhinya rukun dan syarat yang sangat ketat tanpa adanya keraguan (*syubhat*) sedikit pun (Al-Mawardi, 1996). Dalam kasus peretasan aset digital, terdapat beberapa *syubhat* yang menghalangi penerapan sanksi *hadd*. *Syubhat* utama terletak pada konsep "tempat penyimpanan" (*ḥirz*). Para yuris klasik mendefinisikan *ḥirz* sebagai tempat penyimpanan fisik yang terkunci. Menganalogikan sebuah *digital wallet* yang abstrak dengan *ḥirz* fisik adalah sebuah ijtihad yang mengandung keraguan (Audah, 2007).

Syubhat lainnya adalah mengenai cara "mengambil" (*akhż*). Peretasan melibatkan manipulasi kode dan data, bukan tindakan fisik mengambil barang. Perbedaan metode ini, bagi sebagian yuris, cukup untuk menimbulkan keraguan yang menggugurkan sanksi *hadd* (Al-Zuhaili, 2003). Mengingat kaidah fundamental "*idra'ū al-ḥudūd bi al-shubuhāt*" (tolaklah pelaksanaan hukuman *hudūd* apabila terdapat keraguan), maka pandangan yang paling kuat dan hati-hati adalah tidak menerapkan sanksi potong tangan untuk kasus peretasan aset digital.

Namun, tidak diterapkannya sanksi *hadd* sama sekali tidak berarti perbuatan tersebut menjadi boleh atau tidak dihukum. Gugurnya sanksi *hadd* secara otomatis memindahkan perbuatan tersebut ke dalam kategori *jarīmah ta'zīr* (Audah, 2007). Ini menunjukkan fleksibilitas hukum pidana Islam: ketika syarat formal sebuah kejahatan *hadd* tidak terpenuhi, perbuatan tersebut tetap dianggap sebagai tindak pidana serius yang harus dihukum melalui mekanisme *ta'zīr*.

2. Penentuan Kadar Hukuman Ta'zir Berdasarkan Skala Kerugian

Sebagai *jarīmah ta'zīr*, hukuman untuk peretasan diserahkan kepada kebijakan hakim, yang harus mempertimbangkan prinsip proporsionalitas (Kamali, 2000). Faktor utama yang menjadi pertimbangan adalah skala kerugian finansial yang ditimbulkan. Hukuman untuk peretas yang mencuri aset senilai ratusan juta rupiah tentu harus berbeda dengan hukuman untuk sindikat yang membobol bursa dan mencuri triliunan rupiah.

Faktor lain yang memberatkan adalah tingkat kecanggihan serangan, apakah pelaku adalah residivis, dan apakah serangan tersebut menargetkan infrastruktur kritis atau kelompok masyarakat yang rentan (Audah, 2007). Sebaliknya, faktor yang meringankan bisa berupa pelaku yang kooperatif, menunjukkan penyesalan, dan membantu mengembalikan aset yang dicuri. Hukuman *ta'zīr* bisa berupa penjara dengan durasi yang bervariasi, denda, atau kombinasi keduanya.

Tujuan dari penentuan kadar hukuman ini adalah untuk mencapai keadilan yang seimbang. Sanksi harus cukup berat untuk memberikan efek jera bagi pelaku dan calon pelaku lainnya, tetapi juga harus adil dan tidak melampaui batas (*lā tu'zir fawqa al-hadd*) dalam beberapa mazhab (Al-Mawardi, 1996). Fleksibilitas ini memungkinkan hakim untuk merespons setiap kasus secara unik, sesuai dengan tingkat bahaya sosial (*social danger*) yang ditimbulkannya.

3. Pertimbangan Aspek Kerusakan Sistem (Ifsad)

Dalam kasus peretasan skala besar, seperti serangan terhadap sebuah bursa kripto yang menyebabkan bursa tersebut bangkrut dan ribuan penggunanya kehilangan dana, dampaknya bukan hanya kerugian finansial. Dampak lainnya adalah kerusakan kepercayaan terhadap seluruh

ekosistem ekonomi digital. Perbuatan semacam ini memiliki dimensi *ifsād fī al-arḍ* (membuat kerusakan di muka bumi), karena ia merusak tatanan dan stabilitas ekonomi (QS. Al-Ma'idah: 33).

Ketika aspek *ifsād* ini muncul, maka hukuman *ta'zīr* yang dijatuhkan dapat ditingkatkan menjadi sangat berat. Hakim dapat memandang perbuatan tersebut bukan lagi sebagai pencurian biasa, melainkan sebagai kejahatan terorganisir yang mengancam kemaslahatan umum (Audah, 2007). Dalam kasus seperti ini, hukuman penjara yang sangat lama, bahkan hukuman mati dalam kondisi ekstrem yang diatur oleh *siyāsah syar'iyyah* (misalnya jika peretasan tersebut melumpuhkan sistem keuangan negara dan menyebabkan kekacauan massal), dapat menjadi pertimbangan (Hallaq, 2009).

Pertimbangan aspek kerusakan sistem ini penting untuk membedakan antara kejahatan siber biasa dengan kejahatan siber yang memiliki dampak sistemik. Ini menunjukkan bahwa hukum pidana Islam tidak hanya melihat pada kerugian individual, tetapi juga sangat peduli pada dampak sosial yang lebih luas dari sebuah tindak pidana, sejalan dengan *Maqāshid al-Sharī'ah* (Auda, 2008).

4. Prioritas pada Pengembalian Aset kepada Korban

Sama seperti pada kasus penipuan, prioritas utama dalam penanganan kasus peretasan adalah pengembalian aset kepada korban (*restitusi* atau *ḍamān*). Hukuman badan terhadap pelaku menjadi kurang bermakna jika korban tetap menderita kerugian (Ibn Taymiyyah, 1987). Oleh karena itu, seluruh proses penegakan hukum, dari awal investigasi hingga putusan, harus berorientasi pada pemulihan aset (*asset recovery*).

Ini berarti, negara harus mengerahkan seluruh kemampuannya untuk melacak aset kripto yang dicuri, bekerja sama dengan perusahaan analisis *blockchain* dan bursa di seluruh dunia. Setiap aset pelaku yang berhasil disita, baik yang masih dalam bentuk kripto maupun yang sudah diubah menjadi aset lain, harus diprioritaskan untuk dikembalikan kepada korban yang sah (Al-Zuhaili, 2003).

Dalam putusan hakim, perintah untuk mengembalikan aset curian harus menjadi amar yang tidak terpisahkan dari amar pemidanaan. Jika pelaku tidak kooperatif dalam proses pengembalian (misalnya dengan menolak memberikan *private key*), hal tersebut dapat menjadi faktor yang sangat memberatkan dalam penentuan hukuman penjaranya (Audah, 2007). Penekanan pada pemulihan hak korban ini adalah manifestasi dari prinsip keadilan restoratif yang sangat dijunjung tinggi dalam syariah.

D. Pandangan Transaksi Narkotika sebagai Kejahatan Merusak (Mufsid fil-Ardh)

Penggunaan *cryptocurrency* untuk memfasilitasi perdagangan narkotika adalah salah satu bentuk penyalahgunaan teknologi yang paling destruktif. Dari perspektif hukum pidana Islam, kejahatan narkotika tidak dipandang sebagai kejahatan biasa, melainkan sebagai kejahatan serius yang merusak fondasi masyarakat. Sub-bab ini akan menganalisisnya sebagai perbuatan *mufsid fī al-arḍ* dan membahas ketegasan sanksi yang direkomendasikan (Al-Qaradawi, 2001).

1. Dampak Kerusakan Sosial dari Perdagangan Narkotika

Perdagangan dan penyalahgunaan narkotika menimbulkan kerusakan (*mafsadah*) yang multidimensional dan melanggar beberapa tujuan utama syariah (*Maqāshid al-Sharī'ah*) sekaligus. Pertama, ia secara langsung merusak akal (*ḥifẓ al-'aql*) dan jiwa (*ḥifẓ al-nafs*) para penggunanya, menyebabkan kecanduan, penyakit, dan kematian (Auda, 2008). Kedua, ia merusak keturunan (*ḥifẓ al-nasl*) dengan menghancurkan keharmonisan keluarga dan menyebabkan lahirnya generasi yang lemah. Ketiga, ia merusak harta (*ḥifẓ al-māl*) karena para pecandu akan menghabiskan hartanya dan bahkan mungkin mencuri untuk membiayai kecanduannya.

Selain dampak individual, perdagangan narkotika juga memicu kejahatan-kejahatan lain, seperti kekerasan antar geng, korupsi, dan pencucian uang. Ia menciptakan lingkaran setan kejahatan yang mengancam keamanan dan ketertiban umum (*ḥifẓ al-amn*) (BNN, 2022). Mengingat dampak kerusakannya yang begitu luas dan sistemik, para yuris kontemporer sepakat bahwa kejahatan narkotika, terutama bagi para bandar dan pengedar, adalah kejahatan yang sangat berat.

Penggunaan *cryptocurrency* dalam transaksi ini semakin memperparah keadaan, karena ia memberikan lapisan anonimitas yang mempersulit upaya pemberantasan oleh negara (FATF, 2020). Dengan demikian, teknologi yang seharusnya bermanfaat justru disalahgunakan untuk memperlancar perbuatan yang sangat merusak tatanan sosial.

2. Kualifikasi sebagai Kejahatan Berat yang Memerlukan Sanksi Tegas

Mengingat dampak kerusakannya yang masif, para bandar dan pengedar narkotika dapat dikualifikasikan sebagai *mufsid fī al-arḍ* (perusak di muka bumi), sebuah istilah yang digunakan Al-Qur'an untuk kejahatan terberat (QS. Al-Ma'idah: 33). Kualifikasi ini menempatkan kejahatan mereka pada tingkat keseriusan tertinggi dalam kategori *jarīmah ta'zīr*, setara dengan kejahatan *ḥirābah* (terorisme) (Audah, 2007). Mereka bukan lagi sekadar pedagang biasa, melainkan para penjahat yang secara sadar menyebarkan "racun" yang menghancurkan masyarakat dari dalam.

Dengan kualifikasi sebagai *mufsid fī al-arḍ*, mereka layak mendapatkan sanksi *ta'zīr* yang paling tegas dan keras. Tujuannya bukan hanya untuk menghukum, tetapi untuk memberikan efek jera absolut dan untuk membersihkan masyarakat dari bahaya yang mereka timbulkan (Kamali, 2000). Tidak ada ruang untuk toleransi atau keringanan bagi para gembong narkotika yang telah terbukti merusak kehidupan ribuan orang.

Ketegasan ini didasarkan pada prinsip mendahulukan kemaslahatan umum (*maṣlaḥah 'āmah*) di atas kepentingan individu pelaku. Keselamatan jutaan anggota masyarakat dari bahaya narkotika jauh lebih utama daripada hak hidup seorang bandar yang telah terbukti menjadi sumber kerusakan massal (Al-Qaradawi, 2001).

3. Tanggung Jawab Semua Pihak yang Terlibat dalam Transaksi

Dalam jaringan perdagangan narkotika, tanggung jawab pidana tidak hanya dibebankan pada bandar utama. Semua pihak yang secara sadar terlibat dalam rantai pasokan dan transaksi memiliki tingkat pertanggungjawaban, meskipun sanksinya bisa berbeda-beda (Audah, 2007). Ini mencakup kurir yang mengantar barang, perantara yang mengatur transaksi, hingga penyedia jasa penukaran kripto yang secara sadar membantu jaringan tersebut mencuci uangnya.

Prinsip *i'ānah 'alā al-ma'ṣiyah* (membantu dalam kemaksiatan) berlaku bagi semua fasilitator ini. Mereka mungkin tidak secara langsung menjual narkotika, tetapi tanpa peran mereka, jaringan tersebut tidak akan bisa beroperasi (Al-Zuhaili, 2003). Oleh karena itu, mereka juga harus dijatuhi hukuman *ta'zīr* yang berat, yang kadar hukumannya disesuaikan dengan tingkat peran dan keterlibatan mereka dalam jaringan.

Bagi para pembeli atau pengguna, mereka juga melakukan tindak pidana *ta'zīr* karena mengonsumsi zat yang merusak diri sendiri dan karena menciptakan permintaan yang menjadi bahan bakar industri narkotika. Namun, sanksi bagi mereka dapat lebih berorientasi pada rehabilitasi dan pengobatan, terutama jika mereka adalah korban kecanduan, sejalan dengan semangat *iṣlāḥ* (perbaikan) (BNN, 2022).

4. Sanksi Ta'zir yang Dapat Mencakup Hukuman Mati dalam Kondisi Tertentu

Untuk para bandar, pengedar, dan produsen narkotika skala besar yang dikualifikasikan sebagai *mufsid fī al-arḍ*, banyak ulama kontemporer dan lembaga fatwa di dunia yang membolehkan penerapan hukuman mati sebagai bentuk sanksi *ta'zīr* (Al-Qaradawi, 2001). Kebolehan ini didasarkan pada pertimbangan *siyāsah syar'iyyah* untuk melindungi masyarakat dari bahaya yang luar biasa besar. Argumennya adalah bahwa kejahatan mereka setara atau bahkan lebih merusak daripada pembunuhan, karena mereka "membunuh" ribuan orang secara perlahan.

Penerapan hukuman mati ini bukanlah hal yang dianggap enteng dan harus melalui proses pembuktian yang sangat ketat tanpa keraguan sedikit pun (Kamali, 2000). Ia hanya dapat diterapkan oleh negara melalui putusan pengadilan yang sah, dan hanya untuk kasus-kasus yang paling ekstrem (misalnya, gembong jaringan internasional yang bertanggung jawab atas peredaran berton-ton narkotika).

Hukum positif di Indonesia, yang juga menerapkan ancaman hukuman mati untuk kejahatan narkotika (UU No. 35 Tahun 2009), dapat dikatakan sejalan dengan pandangan fikih kontemporer ini. Keduanya sama-sama memandang bahwa ancaman narkotika adalah bahaya luar biasa yang

memerlukan sanksi luar biasa untuk memberantasnya. Ini adalah salah satu contoh di mana hukum positif dan pandangan hukum Islam bertemu pada tingkat sanksi yang paling berat demi menjaga kemaslahatan umum.

Rekomendasi Kebijakan Berbasis Islam

Berdasarkan analisis kasus dari perspektif hukum pidana Islam, kita dapat menarik beberapa benang merah dan merumuskannya menjadi rekomendasi kebijakan yang dapat memperkaya sistem penanggulangan kejahatan ekonomi digital di Indonesia. Rekomendasi ini tidak bertujuan untuk mengganti sistem yang ada, melainkan untuk mengintegrasikan nilai-nilai dan prinsip-prinsip Islam yang relevan ke dalamnya (Hallaq, 2009).

1. Penguatan Aspek Ganti Rugi (Dhaman) bagi Korban

Analisis terhadap semua kasus kejahatan harta (penipuan, pencucian uang, peretasan) secara konsisten menunjukkan bahwa prioritas utama dalam hukum Islam adalah pemulihan hak korban melalui mekanisme ganti rugi (*ḍamān*) atau restitusi (Al-Zuhaili, 2003). Saat ini, hukum acara pidana di Indonesia masih sering menempatkan perampasan aset untuk negara di atas pengembalian kepada korban, terutama dalam kasus kejahatan massal (Putusan MA No. 862 K/Pid.Sus/2023).

Rekomendasi kebijakan yang dapat ditarik adalah perlunya membuat mekanisme hukum dan kelembagaan yang lebih efektif untuk mengelola dan mendistribusikan aset sitaan kepada para korban. Ini bisa berupa pembentukan lembaga wali amanat khusus untuk korban kejahatan massal, atau amandemen pada hukum acara yang mewajibkan hakim untuk memprioritaskan restitusi dalam putusannya (Ibn Taymiyyah, 1987). Semangat keadilan restoratif yang berpusat pada korban ini perlu diperkuat dalam praktik peradilan.

Selain itu, perlu dipikirkan mekanisme kompensasi dari negara bagi korban kejahatan siber dalam kasus di mana aset pelaku tidak mencukupi atau tidak berhasil disita. Ini sejalan dengan konsep *bayt al-māl* yang juga memiliki fungsi sebagai jaring pengaman sosial bagi warga negara yang terzalimi (Chapra, 2000).

2. Penerapan Sanksi Publikasi (Tasyhir) untuk Efek Jera

Efek jera tidak hanya datang dari hukuman penjara. Sanksi sosial dan reputasi sering kali memiliki dampak yang sama kuatnya, terutama bagi pelaku kejahatan kerah putih. Konsep *tasyhīr* dalam fikih, yaitu mempublikasikan identitas dan kejahatan pelaku, dapat diadopsi secara lebih sistematis dalam hukum positif (Al-Mawardi, 1996).

Rekomendasinya adalah membuat sebuah portal data publik yang terintegrasi dan mudah diakses, yang berisi daftar individu dan korporasi yang telah terbukti secara hukum melakukan penipuan keuangan, kejahatan siber, atau pencucian uang. Portal ini akan berfungsi sebagai "daftar hitam" yang dapat menjadi referensi bagi masyarakat sebelum melakukan investasi atau transaksi bisnis. Manfaatnya ganda: memberikan efek jera yang kuat bagi pelaku karena nama baiknya hancur, dan berfungsi sebagai alat pencegahan yang efektif bagi masyarakat (Kamali, 2000).

Implementasi kebijakan ini tentu harus diatur dengan ketat untuk menghindari penyalahgunaan dan fitnah, misalnya data baru dapat dimasukkan setelah putusan pengadilan berkekuatan hukum tetap. Namun, jika diterapkan dengan benar, sanksi publikasi ini dapat menjadi senjata ampuh dalam perang melawan kejahatan ekonomi digital, sejalan dengan semangat *zawājir* (pencegahan) dalam hukum pidana Islam (Audah, 2007).

3. Fleksibilitas Hakim dalam Menentukan Sanksi Ta'zir

Analisis kasus menunjukkan bahwa kejahatan ekonomi digital memiliki spektrum yang sangat luas. Hukum pidana Islam menawarkan prinsip fleksibilitas melalui konsep *ta'zīr*, di mana sanksi dapat disesuaikan dengan kadar kejahatan dan kondisi pelaku (Audah, 2007). Prinsip ini dapat mendorong sistem peradilan pidana nasional untuk bergerak menuju sistem pemidanaan yang lebih personal dan tidak kaku.

Rekomendasi kebijakannya adalah dengan mengembangkan dan menyosialisasikan "pedoman pemidanaan" (*sentencing guidelines*) yang lebih rinci untuk kejahatan siber. Pedoman ini dapat membantu hakim dalam memberikan putusan yang lebih konsisten namun tetap mempertimbangkan faktor-faktor individual (Kamali, 2000). Pedoman ini bisa mencakup skala kerugian, tingkat kecanggihan teknis, peran pelaku

dalam sindikat, dan ada tidaknya upaya pemulihan kerugian sebagai faktor yang memberatkan atau meringankan.

Selain itu, perluasan variasi sanksi di luar penjara dan denda juga perlu didorong. Sanksi kerja sosial, pencabutan hak-hak tertentu (seperti hak mengakses internet atau hak menjalankan usaha), atau hukuman yang bersifat edukatif dapat menjadi alternatif yang lebih efektif untuk beberapa jenis pelaku, sejalan dengan kekayaan variasi hukuman dalam khazanah *ta'zīr* (Al-Mawardi, 1996).

4. Integrasi Prinsip Keadilan Restoratif (Ishlah)

Prinsip utama yang melandasi banyak rekomendasi di atas adalah keadilan restoratif, atau *iṣlāḥ* (perbaikan). Pendekatan ini menggeser fokus dari sekadar menghukum pelaku menjadi upaya untuk memperbaiki kerusakan yang telah terjadi, memulihkan hubungan antara pelaku, korban, dan masyarakat, serta mencegah kejahatan berulang (Auda, 2008).

Rekomendasi kebijakan yang paling mendasar adalah mengubah paradigma penegakan hukum secara bertahap. Dalam kasus-kasus yang memungkinkan, terutama yang melibatkan pelaku muda atau kejahatan dengan skala kecil, mekanisme mediasi penal atau diversi dapat lebih diutamakan (Al-Zuhaili, 2003). Dalam proses ini, pelaku diberi kesempatan untuk bertemu dengan korban (dengan fasilitator), mengakui kesalahannya, dan menyepakati bentuk ganti rugi atau perbaikan yang akan ia lakukan.

Integrasi prinsip *iṣlāḥ* ini akan menghasilkan sistem peradilan yang lebih manusiawi dan efektif dalam jangka panjang. Tujuannya bukan hanya untuk mengisi penjara, tetapi untuk menyembuhkan luka yang ditimbulkan oleh kejahatan dan mereintegrasikan pelaku (setelah menjalani hukumannya dan menunjukkan penyesalan) kembali ke masyarakat sebagai individu yang lebih baik (Hallaq, 2009). Ini adalah tujuan akhir dari keadilan dalam Islam.

Analisis Mendalam Konsep Kunci Bab 9: Aplikasi Analisis Fikih Jinayah pada Kasus Empiris

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk mempraktikkan teori. Jika Bab 5 adalah tentang "bagaimana seharusnya" kejahatan kripto dikualifikasikan, maka Bab 9 adalah tentang "bagaimana kita menganalisis kasus nyata" menggunakan kerangka tersebut. Tujuannya adalah untuk:

1. Menunjukkan Relevansi Praktis Fikih: Membuktikan bahwa konsep-konsep fikih seperti *gharar, tadlis, i'anah 'ala al-ma'siyah*, dan *ta'zir* bukanlah teori usang, melainkan alat analisis yang relevan dan tajam untuk kasus-kasus abad ke-21.
2. Memberikan Penilaian Moral-Yuridis Islam: Memberikan "vonis" atau penilaian dari perspektif Islam terhadap kasus-kasus yang telah diputus oleh pengadilan positif.
3. Membandingkan Logika Hukum: Secara implisit, membandingkan logika hukum positif (yang fokus pada pembuktian unsur pasal) dengan logika hukum Islam (yang fokus pada esensi perbuatan dan pelanggaran terhadap prinsip syariah).
4. Menghasilkan Rekomendasi Berbasis Syariah: Merumuskan rekomendasi konkret mengenai sanksi atau pendekatan keadilan yang diinspirasi oleh prinsip-prinsip fikih jinayah.

Ini adalah proses di mana fakta-fakta dari sebuah kasus nyata "disaring" melalui filter prinsip-prinsip syariah.

Elemen-Elemen Kunci dalam Aplikasi Analisis:

1. Identifikasi Esensi Syar'i dari Kasus: Menerjemahkan deskripsi kasus dari bahasa hukum positif ke dalam terminologi fikih. (Misalnya, "menyebarkan berita bohong yang merugikan konsumen" diterjemahkan menjadi *tadlis*).
2. Penerapan Konsep Fikih yang Relevan: Mengambil konsep-konsep yang telah dibahas (seperti *gharar, maysir, sariqah ta'ziriyah*) dan menggunakannya untuk menganalisis fakta-fakta kasus.

3. Kualifikasi Jarimah: Menegaskan kembali kualifikasi *jarimah* (hampir pasti *Ta'zir*) untuk kasus tersebut.
4. Rekomendasi Sanksi Ta'zir: Mengusulkan jenis sanksi *ta'zir* yang dianggap paling adil dan efektif berdasarkan skala dan dampak kejahatan, dengan fokus pada tujuan *ishlah* (perbaikan) dan *zawajir* (pencegahan).

Analisis Komparatif: Penerapan Analisis Fikih pada Berbagai Jenis Kasus

Tabel berikut membedah bagaimana analisis fikih jinayah diterapkan secara spesifik pada studi kasus yang telah dibahas di Bab 8.

Studi Kasus (dari Bab 8)	Konsep Fikih Kunci yang Diterapkan	Hasil Analisis dari Perspektif Islam	Rekomendasi Sanksi Ta'zir yang Sesuai
Kasus Penipuan Investasi (*Robot Trading*)	*Gharar Fahish* (Ketidakpastian Ekstrem) & *Tadlis* (Penipuan Informasi).	Perbuatan ini adalah bentuk penipuan terorganisir yang secara sengaja menyembunyikan risiko dan menjual ilusi keuntungan pasti. Ini adalah pelanggaran berat terhadap prinsip larangan memakan harta secara batil.	Prioritas Utama: Ganti rugi penuh kepada korban (*dhaman*). Sanksi Tambahan: Hukuman penjara (*habs*) yang setimpal dan publikasi pelaku (*tasyhir*) untuk melindungi masyarakat.
Kasus Pencucian Uang (*Influencer*)	*I'anah 'ala al-Ma'siyah* (Bantuan terhadap Kejahatan) & Penerimaan Harta Haram.	*Influencer* yang menerima dana dari hasil kejahatan (judi *online*) dan memamerkannya adalah pihak yang turut serta dalam dosa dan kejahatan. Ia membantu menormalkan dan mempromosikan sumber haram tersebut.	Kewajiban Utama: Mengembalikan seluruh harta yang diterima dari sumber haram. Sanksi Tambahan: Hukuman penjara yang mendidik dan larangan melakukan aktivitas promosi serupa di masa depan.
Kasus Peretasan (*Hacking*)	*Sariqah Ta'ziriyah* (Pencurian Ta'zir) & *Ifsad* (Perusakan).	Ini adalah pencurian, tetapi tidak memenuhi syarat *hudud*. Namun, karena merusak sistem dan kepercayaan publik, ia juga mengandung unsur *ifsad*. Ini adalah kejahatan ganda: pencurian dan perusakan.	Prioritas Utama: Pengembalian aset kepada korban. Sanksi Tambahan: Hukuman penjara yang berat, sepadan dengan skala kerugian dan tingkat kerusakan sistem yang ditimbulkan.
Kasus Transaksi Narkotika	*Ifsad fil-Ardh* (Perusakan di Muka Bumi) & Pelanggaran *Hifzh al-'Aql* (Perlindungan Akal).	Ini adalah salah satu kejahatan paling serius karena dampaknya merusak individu (akal dan jiwa) dan masyarakat secara luas. Penggunaan kripto hanya sebagai alat, tidak mengubah substansi kejahatannya.	Sanksi *ta'zir* yang paling tegas dan berat, yang dalam pandangan sebagian ulama dan hukum positif dapat mencakup hukuman mati, untuk melindungi masyarakat dari bahaya yang lebih besar.

Kontribusi Konsep Aplikasi Analisis dalam Bab 9:

Konsep ini adalah pembuktian akhir dari relevansi hukum pidana Islam.

1. Menghidupkan Fikih: Bab ini menunjukkan bahwa fikih bukanlah sekadar teks-teks kuno, melainkan sebuah metodologi analisis yang hidup dan dapat diterapkan pada masalah-masalah paling modern sekalipun.
2. Memberikan Perspektif Alternatif: Ia menawarkan cara pandang yang berbeda dari hukum positif. Jika hukum positif berhenti pada "apakah unsur pasal terpenuhi?", analisis fikih melangkah lebih jauh ke "apakah prinsip keadilan, kemaslahatan, dan larangan syariah dilanggar?".
3. Menghasilkan Rekomendasi Unik: Analisis ini menghasilkan rekomendasi yang mungkin tidak menjadi prioritas utama dalam hukum positif, seperti penekanan yang sangat kuat pada ganti rugi korban (*dhaman*) sebagai tujuan utama pemidanaan, dan penggunaan sanksi reputasi seperti *tasyhir*.
4. Menjadi Puncak Argumen Buku: Bab ini secara definitif menjawab pertanyaan penelitian utama buku ini: "Bagaimana kejahatan ekonomi digital menggunakan *cryptocurrency* dapat dikaji dan ditanggulangi dari perspektif hukum pidana Islam?".

Secara ringkas, Bab 9 adalah "ruang praktik" di mana seorang ahli fikih mengambil laporan kasus dari pengadilan negeri (Bab 8) dan menulis sebuah "opini hukum syariah" atau "analisis yuridis Islam" yang mendalam. Ini menunjukkan bagaimana dua sistem hukum dapat melihat fakta yang sama namun menganalisisnya dengan logika dan prioritas yang sedikit berbeda, meskipun sering kali sampai pada kesimpulan yang serupa mengenai tercelanya perbuatan tersebut.

BAB 10

Peran Lembaga Penegak Hukum dan Keuangan

Setelah menganalisis kerangka hukum dan studi kasus, pemahaman yang komprehensif mengenai penanggulangan kejahatan ekonomi digital menuntut adanya analisis terhadap para aktor kelembagaan yang berada di garis depan. Hukum tidak berjalan di ruang hampa; ia diimplementasikan, ditafsirkan, dan ditegakkan oleh lembaga-lembaga negara (Hadjon, 1987). Bab 10 ini akan memetakan peran, fungsi, dan tantangan yang dihadapi oleh lembaga-lembaga kunci di Indonesia, mulai dari kepolisian sebagai penyidik, kejaksaan sebagai penuntut, PPATK sebagai unit intelijen keuangan, OJK dan BI sebagai penjaga stabilitas sistem keuangan, hingga Bappebti sebagai regulator pasar. *Research gap* yang diisi adalah kurangnya pembahasan terpadu yang melihat dinamika antarlembaga dan tantangan spesifik yang dihadapi masing-masing institusi dalam konteks kejahatan *cryptocurrency*. Pertanyaan penelitian utama yang akan dijawab adalah: Bagaimana peran dan fungsi masing-masing lembaga penegak hukum dan keuangan dalam menanggulangi kejahatan kripto, serta tantangan dan strategi peningkatan kapasitas apa yang paling mendesak untuk diatasi?

A. Kepolisian Negara Republik Indonesia (Polri)

Sebagai garda terdepan dalam penegakan hukum pidana, Kepolisian Negara Republik Indonesia (Polri) memegang peran sentral dalam memberantas kejahatan siber. Melalui direktorat khususnya, Polri bertugas melakukan penyelidikan dan penyidikan (Polri, 2021). Sub-bab ini akan mengupas peran Direktorat Tindak Pidana Siber (Dittipidsiber), tantangan investigasi lintas batas yang dihadapinya, serta urgensi peningkatan kapasitas forensik dan kerja sama dengan komunitas ahli.

1. Peran Direktorat Tindak Pidana Siber (Dittipidsiber)

Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri adalah ujung tombak Polri dalam menangani kejahatan di dunia maya. Dibentuk untuk merespons meningkatnya ancaman siber, Dittipidsiber memiliki yurisdiksi untuk menyelidiki semua tindak pidana yang menggunakan teknologi informasi sebagai medium atau target, termasuk kejahatan yang melibatkan *cryptocurrency* (Peraturan Kapolri No. 6 Tahun 2019). Peran utamanya mencakup patroli siber untuk mendeteksi aktivitas ilegal, menerima laporan dari masyarakat, melakukan penyelidikan

untuk mengidentifikasi pelaku, hingga melakukan penyidikan untuk mengumpulkan alat bukti yang sah.

Dalam kasus kejahatan kripto, peran Dittipidsiber sangat luas. Mereka menyelidiki kasus penipuan investasi online, peretasan akun bursa, pencurian aset digital, hingga penggunaan kripto untuk transaksi ilegal seperti narkotika dan pendanaan terorisme (Polri, 2021). Tim penyidik di Dittipidsiber tidak hanya terdiri dari polisi dengan latar belakang hukum, tetapi juga diperkuat oleh personel dengan keahlian di bidang teknologi informasi, forensik digital, dan analisis data. Mereka adalah pihak pertama yang melakukan analisis teknis, melacak jejak digital, dan berupaya mengungkap identitas pelaku yang bersembunyi di balik anonimitas.

Keberhasilan dalam mengungkap kasus-kasus besar seperti penipuan robot trading atau penangkapan afiliator *binary option* menunjukkan peran vital Dittipidsiber. Mereka bertindak sebagai "penerjemah" antara dunia siber yang kompleks dan dunia hukum yang formal, mengubah jejak-jejak digital yang abstrak menjadi berkas perkara yang siap untuk dilimpahkan ke kejaksaan (Laporan Media, Tempo, 2022).

2. Tantangan dalam Penyelidikan dan Penyidikan Lintas Batas

Tantangan terbesar yang dihadapi Dittipidsiber adalah sifat kejahatan siber yang tidak mengenal batas negara (*borderless*). Sangat umum ditemukan kasus di mana pelaku berada di satu negara, server yang digunakan berada di negara kedua, dan korban berada di Indonesia (Interpol, 2022). Situasi ini menciptakan tantangan yurisdiksi dan pengumpulan bukti yang luar biasa rumit. Penyidik Polri tidak memiliki kewenangan untuk melakukan penyitaan atau penangkapan di negara lain.

Untuk mendapatkan bukti dari server atau perusahaan teknologi yang berlokasi di luar negeri (misalnya, data dari penyedia layanan email atau media sosial), Polri harus menempuh jalur Bantuan Hukum Timbal Balik (*Mutual Legal Assistance* - MLA). Proses ini bersifat formal antarnegara, dikoordinasikan melalui Kementerian Hukum dan HAM, dan sering kali memakan waktu berbulan-bulan bahkan bertahun-tahun (Kementerian Hukum dan HAM, 2019). Keterlambatan ini memberikan waktu yang sangat panjang bagi pelaku untuk menghilangkan jejak atau memindahkan asetnya.

Selain itu, tidak semua negara memiliki perjanjian MLA dengan Indonesia atau bersedia bekerja sama. Beberapa negara bahkan menjadi "surga" bagi para penjahat siber karena lemahnya penegakan hukum atau keengganan untuk bekerja sama (FATF, 2021). Tantangan lintas batas ini sering kali menjadi tembok penghalang yang membuat banyak kasus kejahatan siber, terutama peretasan, sulit untuk diungkap tuntas hingga ke pelakunya.

3. Peningkatan Kapasitas Penyidik dalam Forensik Digital

Kejahatan *cryptocurrency* terus berevolusi dengan sangat cepat. Para pelaku terus mengembangkan teknik-teknik baru untuk mengaburkan jejak, seperti penggunaan *mixer*, *privacy coins*, dan platform Keuangan Terdesentralisasi (DeFi) (Chainalysis, 2023). Untuk mengimbangi hal ini, peningkatan kapasitas penyidik dalam bidang forensik digital dan analisis *blockchain* menjadi sebuah keharusan yang tidak bisa ditawar.

Peningkatan kapasitas ini mencakup beberapa aspek. Pertama, pelatihan berkelanjutan. Penyidik siber harus secara rutin mendapatkan pelatihan mengenai teknologi *blockchain* terbaru, alat-alat analisis *on-chain*, dan modus-modus operandi kejahatan kripto yang sedang tren (Polri, 2021). Kedua, investasi pada teknologi. Dittipidsiber perlu dilengkapi dengan perangkat keras dan perangkat lunak forensik tercanggih, termasuk akses ke *platform* analisis *blockchain* komersial (seperti Chainalysis, Elliptic, atau TRM Labs) yang memiliki database alamat berisiko dan alat visualisasi transaksi.

Ketiga, pengembangan sumber daya manusia. Polri perlu terus merekrut talenta-talenta terbaik di bidang IT untuk menjadi penyidik siber. Pemberian jalur karir yang jelas, insentif yang menarik, dan lingkungan kerja yang mendukung inovasi menjadi kunci untuk mempertahankan para ahli ini di dalam institusi (Pratama, 2020). Tanpa peningkatan kapasitas yang konstan, penyidik akan selalu tertinggal satu langkah di belakang para penjahat.

4. Kerjasama dengan Komunitas Kripto (White Hat Hackers)

Dalam menghadapi kejahatan siber yang sangat teknis, Polri tidak bisa bekerja sendirian. Menjalin kerja sama dengan komunitas ahli di luar

institusi adalah sebuah strategi yang cerdas dan efektif (Interpol, 2022). Salah satu komunitas yang paling potensial untuk diajak bekerja sama adalah para peretas etis (*white hat hackers*) dan para ahli keamanan siber di sektor swasta, termasuk para pengembang dan analis dalam komunitas kripto itu sendiri.

Para ahli ini sering kali memiliki pengetahuan yang sangat mendalam dan *up-to-date* mengenai kerentanan sistem, cara kerja serangan, dan teknik pelacakan aset yang mungkin belum dikuasai sepenuhnya oleh penyidik. Mereka dapat memberikan wawasan berharga, membantu menganalisis *malware*, atau bahkan membantu melacak aliran dana curian secara pro bono atau melalui mekanisme kemitraan formal (Chainalysis, 2023). Di tingkat global, sudah banyak contoh di mana peretasan besar berhasil diungkap berkat bantuan dari para analis *blockchain* independen.

Untuk memformalkan kerja sama ini, Polri dapat mengembangkan program seperti *bug bounty* atau menciptakan sebuah forum komunikasi yang aman antara Dittipidsiber dan komunitas ahli keamanan siber. Membangun kepercayaan dan hubungan baik dengan komunitas ini akan menjadi aset yang tak ternilai, mengubah mereka dari pengamat menjadi mitra strategis dalam perang melawan kejahatan siber (Pratama, 2020).

B. Kejaksaan Agung

Setelah proses penyidikan oleh Polri selesai, berkas perkara dilimpahkan kepada Kejaksaan Agung. Sebagai penuntut umum, Kejaksaan memegang peran krusial dalam menentukan apakah sebuah kasus layak dibawa ke pengadilan dan bagaimana cara membuktikannya di hadapan hakim (Kejaksaan RI, 2020). Sub-bab ini akan membahas peran jaksa, tantangan dalam pembuktian niat jahat, dan pentingnya spesialisasi jaksa siber.

1. Peran Jaksa dalam Penuntutan Kasus Kejahatan Kripto

Peran jaksa dimulai sejak tahap pra-penuntutan, di mana jaksa (jaksa peneliti) meneliti kelengkapan berkas perkara yang diserahkan oleh penyidik Polri. Jaksa harus memastikan bahwa bukti-bukti yang dikumpulkan sudah cukup kuat (baik secara formil maupun materiil) untuk membuktikan semua unsur pasal yang didakwakan (UU No. 8 Tahun 1981 tentang Hukum Acara Pidana). Dalam kasus kejahatan kripto yang kompleks, peran jaksa peneliti

sangat vital untuk memberikan petunjuk kepada penyidik jika ada bukti-bukti yang masih kurang, misalnya perlu adanya keterangan ahli forensik digital atau analisis aliran dana yang lebih mendalam.

Setelah berkas dinyatakan lengkap (P-21), jaksa penuntut umum akan menyusun surat dakwaan. Penyusunan dakwaan dalam kasus kejahatan kripto memerlukan kecermatan tinggi. Jaksa harus memilih pasal-pasal yang paling relevan (misalnya, kombinasi KUHP, UU ITE, dan UU TPPU) dan merumuskan dakwaan secara cermat, jelas, dan lengkap (Putusan MA No. 862 K/Pid.Sus/2023). Di persidangan, jaksa bertugas untuk membuktikan dakwaannya dengan menghadirkan saksi-saksi dan alat bukti, termasuk menjelaskan bukti digital yang rumit kepada majelis hakim yang mungkin tidak memiliki latar belakang teknis.

Pada tahap akhir, jaksa akan mengajukan surat tuntutan (requisitor) yang berisi analisis yuridis terhadap fakta-fakta persidangan dan tuntutan hukuman pidana bagi terdakwa. Tuntutan ini harus didasarkan pada bukti-bukti yang terungkap dan mempertimbangkan rasa keadilan masyarakat (Kejaksaan RI, 2020). Peran jaksa, dari awal hingga akhir, adalah sebagai "arsitek" dari proses pembuktian hukum di pengadilan.

2. Kompleksitas Pembuktian Niat Jahat (Mens Rea)

Salah satu tantangan terbesar bagi jaksa dalam kasus kejahatan ekonomi digital adalah membuktikan unsur kesalahan atau niat jahat (*mens rea*) dari terdakwa. Dalam banyak kasus, terdakwa akan berdalih bahwa mereka tidak berniat menipu, melainkan hanya mengalami kegagalan bisnis, atau bahwa mereka tidak memahami teknologi yang mereka gunakan (Chazawi, 2002). Mematahkan pembelaan semacam ini memerlukan kelihaian jaksa dalam merangkai bukti-bukti tidak langsung (*circumstantial evidence*).

Misalnya, dalam kasus penipuan investasi, jaksa tidak bisa hanya bergantung pada pengakuan terdakwa. Jaksa harus menunjukkan adanya pola perilaku yang mengindikasikan niat jahat sejak awal. Ini bisa berupa bukti bahwa terdakwa menggunakan identitas palsu, membuat klaim yang secara objektif tidak mungkin benar, atau secara diam-diam mentransfer dana investor ke rekening pribadi (Putusan PN Jakarta Barat No. 711/

Pid.Sus/2022). Dalam kasus peretasan, niat jahat dapat dibuktikan dari penggunaan *malware* atau alat-alat peretasan yang jelas-jelas dirancang untuk tujuan kriminal.

Pembuktian *mens rea* menjadi semakin rumit dalam kasus pencucian uang, di mana jaksa harus membuktikan bahwa terdakwa "mengetahui atau patut menduga" bahwa harta yang ia kelola berasal dari tindak pidana (UU No. 8 Tahun 2010). Jaksa harus membangun argumen berdasarkan profil terdakwa, kewajaran transaksi, dan adanya "bendera merah" (*red flags*) yang seharusnya membuat terdakwa curiga. Kemampuan jaksa untuk membangun argumen logis dari serangkaian bukti tidak langsung inilah yang sering kali menjadi penentu kemenangan dalam persidangan.

3. Tuntutan Perampasan Aset Digital

Dalam kasus kejahatan ekonomi, tuntutan jaksa tidak boleh hanya terbatas pada hukuman penjara atau denda. Tuntutan yang paling penting untuk memulihkan kerugian dan memberikan efek jera adalah perampasan aset (UU No. 8 Tahun 2010). Jaksa yang menangani kasus TPPU memiliki kewenangan untuk menuntut agar seluruh aset yang merupakan hasil kejahatan atau terkait dengannya dirampas, baik untuk dikembalikan kepada korban maupun untuk negara.

Dalam konteks aset digital, tuntutan ini memiliki kompleksitas teknis. Jaksa harus mampu menyajikan bukti hasil pelacakan aset (*asset tracing*) yang jelas di hadapan hakim, menunjukkan aliran dana dari kejahatan asal hingga menjadi aset kripto atau aset lain yang dimiliki terdakwa (PPATK, 2022). Jaksa harus bisa menjelaskan kepada hakim bagaimana cara menyita dan mengelola aset kripto, yang mungkin memerlukan kerja sama dengan ahli atau lembaga kustodian.

Selain itu, jaksa juga harus mengambil posisi yang jelas mengenai status aset rampasan tersebut. Apakah jaksa akan menuntut agar aset dikembalikan kepada korban, atau dirampas untuk negara? Pilihan ini memiliki implikasi hukum dan keadilan yang besar, seperti yang terlihat dalam perbedaan putusan di berbagai tingkat peradilan kasus Doni Salmanan (Putusan MA No. 862 K/Pid.Sus/2023). Jaksa harus mendasarkan

tuntutannya pada analisis yang cermat terhadap kemungkinan teknis pendistribusian kepada korban, skala kejahatan, dan yurisprudensi yang ada, sambil tetap memperjuangkan rasa keadilan bagi para korban.

4. Kebutuhan Spesialisasi Jaksa di Bidang Kejahatan Siber

Mengingat kompleksitas teknis dan yuridis dari kejahatan *cryptocurrency*, kebutuhan akan jaksa spesialis di bidang kejahatan siber menjadi sangat mendesak. Seorang jaksa yang terbiasa menangani kasus-kasus konvensional mungkin akan kewalahan ketika dihadapkan pada berkas perkara yang penuh dengan istilah teknis, analisis *blockchain*, dan bukti forensik digital (Kejaksaan RI, 2020). Spesialisasi akan memungkinkan jaksa untuk mengembangkan pemahaman yang mendalam dan intuisi yang tajam dalam menangani kasus-kasus ini.

Spesialisasi ini dapat dibangun melalui beberapa cara. Pertama, jalur pendidikan dan pelatihan khusus yang intensif bagi para jaksa mengenai hukum siber, teknologi *blockchain*, dan teknik-teknik pembuktian digital. Pelatihan ini harus bersifat berkelanjutan untuk mengikuti perkembangan teknologi (Pratama, 2020). Kedua, pembentukan unit atau satuan tugas khusus di dalam Kejaksaan yang didedikasikan untuk menangani kejahatan siber dan TPPU, diisi oleh jaksa-jaksa yang telah mendapatkan pelatihan khusus.

Ketiga, rotasi dan penempatan strategis. Jaksa yang menunjukkan minat dan bakat di bidang ini harus diberikan kesempatan untuk menangani lebih banyak kasus siber agar pengalaman mereka terasah. Dengan adanya korps jaksa spesialis siber yang andal, Kejaksaan akan lebih siap untuk berdebat secara efektif dengan pengacara terdakwa yang mungkin menyewa ahli IT mahal, dan mampu menyajikan kasus yang solid dan meyakinkan di hadapan hakim (Chazawi, 2002).

C. Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK)

PPATK adalah lembaga sentral dalam rezim Anti-Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU-PPT) di Indonesia. Sebagai unit intelijen keuangan (*Financial Intelligence Unit* - FIU), PPATK tidak melakukan

penyidikan, tetapi perannya dalam mendeteksi dan mencegah aliran dana ilegal sangat krusial (PPATK, 2022). Sub-bab ini akan membahas fungsi intelijen PPATK, penggunaan teknologi, kerja sama internasional, dan tantangan yang dihadapinya.

1. Fungsi Intelijen Keuangan dalam Mendeteksi Transaksi Mencurigakan

Fungsi utama PPATK adalah menerima, menganalisis, dan menyebarluaskan informasi intelijen keuangan. Sumber informasi utamanya adalah laporan dari Pihak Pelapor, yang mencakup bank, perusahaan sekuritas, dan Pedagang Fisik Aset Kripto (PFAK) (UU No. 8 Tahun 2010). PPATK menerima berbagai jenis laporan, termasuk Laporan Transaksi Keuangan Mencurigakan (LTKM), Laporan Transaksi Keuangan Tunai (LTKT), dan Laporan Transaksi Penyedia Jasa Keuangan.

Ketika PPATK menerima laporan transaksi kripto yang mencurigakan dari sebuah PFAK, para analisnya akan mulai bekerja. Mereka akan menganalisis transaksi tersebut dalam konteks yang lebih luas, membandingkannya dengan profil nasabah, riwayat transaksinya, dan menghubungkannya dengan data-data lain yang dimiliki PPATK (PPATK, 2022). Tujuannya adalah untuk mengidentifikasi apakah transaksi tersebut merupakan indikasi adanya tindak pidana, seperti penipuan, pencucian uang, atau pendanaan terorisme.

Jika hasil analisis menunjukkan adanya indikasi kuat tindak pidana, PPATK akan menyusun "Hasil Analisis" dan menyerahkannya kepada lembaga penegak hukum yang berwenang (Polri, Kejaksaan, KPK, atau BNN). Hasil Analisis ini berfungsi sebagai informasi intelijen awal yang sangat berharga, yang memungkinkan penegak hukum untuk memulai penyelidikan dengan data yang sudah matang (PPATK, 2022). Dengan demikian, PPATK berperan sebagai "mata dan telinga" negara dalam sistem keuangan.

2. Analisis Big Data untuk Mengidentifikasi Pola Pencucian Uang

Dengan jutaan laporan transaksi yang masuk setiap tahun, PPATK mengelola sebuah basis data yang sangat besar (*big data*). Untuk dapat mengolah data sebanyak ini secara efektif, PPATK semakin bergantung

pada penggunaan teknologi canggih seperti analisis *big data* dan kecerdasan buatan (*Artificial Intelligence* - AI) (PPATK, 2022). Teknologi ini memungkinkan PPATK untuk beralih dari pendekatan reaktif (menganalisis laporan yang masuk) ke pendekatan proaktif (mencari pola-pola anomali).

Sistem AI dapat dilatih untuk mengenali pola-pola pencucian uang yang umum, seperti *structuring* (memecah transaksi besar menjadi transaksi kecil untuk menghindari pelaporan), penggunaan jaringan rekening nomine yang kompleks, atau pola aliran dana yang tidak wajar (FATF, 2020). Dalam konteks kripto, analisis ini dapat diperluas untuk mengidentifikasi pola *on-chain*, misalnya ketika sejumlah besar dana dari berbagai alamat tiba-tiba terkonsolidasi dan dikirim ke alamat yang masuk daftar hitam.

Dengan menggunakan analisis *big data*, PPATK dapat mengidentifikasi jaringan kejahatan yang mungkin tidak terdeteksi melalui analisis kasus per kasus. Kemampuan untuk melihat "gambaran besar" dari aliran dana di seluruh sistem keuangan, termasuk di ekosistem kripto, menjadikan PPATK sebagai salah satu aktor paling strategis dalam pemberantasan kejahatan ekonomi (PPATK, 2022).

3. Kerjasama dengan Financial Intelligence Unit (FIU) Negara Lain

Pencucian uang dan pendanaan terorisme adalah kejahatan transnasional. Oleh karena itu, kerja sama internasional adalah kunci bagi efektivitas PPATK. PPATK merupakan anggota dari Egmont Group, sebuah jaringan informal yang terdiri dari lebih dari 160 FIU di seluruh dunia (Egmont Group, 2023). Keanggotaan ini memungkinkan PPATK untuk bertukar informasi intelijen keuangan dengan mitranya di negara lain secara cepat dan aman melalui platform Egmont Secure Web (ESW).

Kerja sama ini sangat vital dalam melacak aliran dana kripto yang lintas batas. Misalnya, jika PPATK mendeteksi adanya transfer kripto dalam jumlah besar dari bursa Indonesia ke sebuah bursa di Singapura yang diduga terkait pencucian uang, PPATK dapat segera mengirimkan permintaan informasi kepada FIU Singapura (PPATK, 2022). FIU Singapura kemudian dapat menindaklanjuti permintaan tersebut dengan meminta data dari bursa di negaranya. Pertukaran informasi ini memungkinkan pelacakan aset yang seamless melintasi yurisdiksi.

Selain pertukaran informasi spontan, PPATK juga aktif terlibat dalam proyek-proyek tipologi pencucian uang bersama FIU lain. Mereka berbagi pengetahuan dan pengalaman mengenai modus-modus operandi terbaru, termasuk yang menggunakan *cryptocurrency* (FATF, 2021). Kolaborasi global ini memastikan bahwa PPATK dan mitranya di seluruh dunia dapat terus beradaptasi dan selangkah lebih maju dalam menghadapi jaringan kejahatan keuangan internasional.

4. Tantangan dalam Menganalisis Transaksi di Jaringan Terdesentralisasi

Tantangan terbesar yang dihadapi PPATK dan semua FIU di dunia saat ini adalah kebangkitan Keuangan Terdesentralisasi (DeFi). Berbeda dengan transaksi melalui bursa terpusat (CeFi) di mana ada entitas (PFAK) yang dapat diwajibkan untuk melapor, transaksi di platform DeFi terjadi secara *peer-to-peer* melalui *smart contract* tanpa adanya perantara (Schär, 2021). Tidak ada "Pihak Pelapor" dalam ekosistem DeFi.

Hal ini menciptakan "lubang hitam" dalam pengawasan. Pelaku kejahatan dapat menggunakan *decentralized exchanges* (DEX), protokol *lending*, atau *mixer* terdesentralisasi untuk mencuci uang tanpa melalui entitas yang dapat diawasi oleh PPATK (Chainalysis, 2023). Pelacakan transaksi di DeFi jauh lebih sulit karena identitas pengguna sepenuhnya anonim dan hanya diwakili oleh alamat *pseudonymous*.

Untuk mengatasi tantangan ini, PPATK dan regulator global sedang menjajaki pendekatan baru, sejalan dengan rekomendasi FATF. Salah satunya adalah dengan fokus mengawasi titik masuk dan keluar (*on-ramp* dan *off-ramp*), yaitu ketika dana bergerak dari sistem keuangan tradisional ke DeFi atau sebaliknya (FATF, 2021). Pendekatan lainnya adalah dengan mengembangkan alat analisis *on-chain* yang lebih canggih yang dapat mengelompokkan alamat-alamat yang kemungkinan besar dikendalikan oleh satu entitas yang sama, bahkan di lingkungan DeFi. Namun, ini tetap menjadi tantangan regulasi dan teknologi yang paling signifikan di dekade ini.

D. Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI)

Meskipun perdagangan aset kripto diawasi oleh Bappebti, OJK dan BI sebagai otoritas utama di sektor jasa keuangan dan sistem pembayaran memiliki peran penting dalam mitigasi risiko dan menjaga stabilitas makro. Sub-bab ini akan membahas peran pengawasan OJK dan BI, upaya edukasi publik, pengembangan Rupiah Digital, dan kolaborasi antarlembaga (OJK, 2022; Bank Indonesia, 2022).

1. Pengawasan Sektor Jasa Keuangan dari Paparan Risiko Kripto

Peran utama OJK dan BI adalah memastikan bahwa lembaga jasa keuangan yang mereka awasi (bank, perusahaan asuransi, perusahaan pembiayaan, dll.) tidak terpapar pada risiko yang berlebihan dari volatilitas dan aktivitas ilegal di pasar kripto. OJK, misalnya, secara tegas melarang lembaga jasa keuangan untuk menggunakan, memasarkan, dan/atau memfasilitasi perdagangan aset kripto (OJK, 2022). Larangan ini bertujuan untuk melindungi integritas sistem keuangan formal dari risiko spekulatif dan risiko pencucian uang yang melekat pada aset kripto.

BI juga mengambil sikap yang sama tegasnya. BI secara konsisten menegaskan bahwa *cryptocurrency* bukanlah alat pembayaran yang sah di Indonesia dan melarang semua penyelenggara jasa sistem pembayaran (seperti penyedia dompet digital atau gerbang pembayaran) untuk memproses transaksi menggunakan aset kripto (Bank Indonesia, 2018). Sikap ini penting untuk menjaga kedaulatan Rupiah sebagai satu-satunya alat pembayaran yang sah dan untuk mencegah risiko volatilitas kripto masuk ke dalam sistem pembayaran ritel.

Pengawasan ini menciptakan "dinding api" (*firewall*) antara sistem keuangan formal yang teregulasi dengan ekosistem kripto yang lebih liar. Meskipun demikian, OJK dan BI tetap harus waspada terhadap risiko tidak langsung, misalnya ketika nasabah bank menggunakan dana pinjaman untuk berspekulasi di pasar kripto, yang dapat meningkatkan risiko kredit macet (Bank Indonesia, 2022).

2. Peringatan kepada Masyarakat tentang Risiko Investasi Kripto

Selain pengawasan internal, OJK dan BI, sering kali melalui Satgas Waspada Investasi (SWI) di mana mereka menjadi anggotanya, memiliki peran penting dalam melakukan edukasi dan memberikan peringatan kepada masyarakat. Kedua lembaga ini secara rutin mengeluarkan siaran pers, unggahan media sosial, dan menyelenggarakan seminar untuk mengingatkan masyarakat tentang risiko tinggi yang terkait dengan investasi aset kripto (OJK, 2022).

Peringatan ini biasanya mencakup beberapa poin utama. Pertama, risiko volatilitas harga yang ekstrem, di mana nilai aset kripto dapat anjlok secara drastis dalam waktu singkat. Kedua, risiko penipuan, di mana banyak penawaran investasi kripto yang ternyata adalah skema Ponzi atau penipuan lainnya. Ketiga, risiko keamanan siber, seperti peretasan akun bursa atau dompet digital. Keempat, kurangnya perlindungan konsumen, karena industri ini belum sepenuhnya matang dan mekanisme penyelesaian sengketa sering kali tidak jelas (Bank Indonesia, 2022).

Peran edukasi dan komunikasi publik ini sangat krusial. Dalam lanskap di mana promosi investasi kripto yang menyesatkan sangat masif di media sosial, suara otoritas seperti OJK dan BI menjadi penyeimbang yang penting. Upaya mereka untuk terus-menerus "mengingatkan" masyarakat adalah garda pertahanan pertama untuk mencegah lebih banyak korban berjatuhan.

3. Pengembangan Rupiah Digital (CBDC) sebagai Alternatif

Sebagai respons strategis jangka panjang terhadap fenomena aset digital, Bank Indonesia saat ini sedang dalam tahap pengembangan Rupiah Digital, yang merupakan salah satu bentuk *Central Bank Digital Currency* (CBDC). Proyek yang diberi nama Proyek Garuda ini bertujuan untuk menciptakan versi digital dari mata uang Rupiah yang diterbitkan dan dijamin oleh BI (Bank Indonesia, 2022). Rupiah Digital dirancang untuk menjadi satu-satunya alat pembayaran digital yang sah di Indonesia, melengkapi uang kartal dan uang elektronik yang sudah ada.

Pengembangan Rupiah Digital memiliki beberapa tujuan strategis. Pertama, untuk menyediakan alat pembayaran digital yang aman, efisien,

dan bebas risiko kredit, sebagai alternatif dari *stablecoin* swasta atau aset kripto lainnya. Kedua, untuk memperluas inklusi keuangan dengan menyediakan akses ke sistem pembayaran modern bagi masyarakat yang belum terjangkau oleh perbankan. Ketiga, untuk meningkatkan efisiensi dalam transaksi wholesale antar bank (Bank Indonesia, 2022).

Dengan mengembangkan Rupiah Digital, BI tidak hanya mencoba untuk bersaing, tetapi juga untuk membentuk masa depan ekosistem keuangan digital Indonesia. Jika berhasil diimplementasikan, Rupiah Digital dapat mengurangi daya tarik penggunaan aset kripto untuk tujuan pembayaran dan memberikan BI alat kebijakan moneter dan pengawasan yang lebih efektif di era digital (Auer & Böhme, 2020).

4. Kolaborasi dengan BAPPEBTI dalam Pengawasan

Meskipun terdapat pembagian yurisdiksi yang jelas—BI untuk sistem pembayaran, OJK untuk jasa keuangan, dan Bappebti untuk perdagangan komoditas kripto—kolaborasi antar ketiganya menjadi semakin tak terhindarkan. Risiko dalam ekosistem kripto dapat dengan mudah merembet dari satu sektor ke sektor lainnya (FATF, 2021). Oleh karena itu, diperlukan sebuah forum koordinasi yang kuat di antara para regulator ini.

Kolaborasi ini dapat berbentuk pertukaran informasi secara rutin. Bappebti dapat memberikan data dan wawasan mengenai perkembangan di pasar kripto kepada OJK dan BI, sementara OJK dan BI dapat memberikan informasi mengenai potensi risiko sistemik yang mereka lihat dari sisi perbankan dan sistem pembayaran (OJK, 2022). Mereka juga dapat berkoordinasi dalam mengeluarkan peringatan dan pernyataan publik agar pesan yang disampaikan kepada masyarakat seragam dan tidak membingungkan.

Ke depan, seiring dengan semakin kaburnya batas antara jasa keuangan, sistem pembayaran, dan investasi komoditas (misalnya, dengan munculnya produk *staking* atau *lending* kripto yang mirip produk perbankan), kolaborasi ini perlu diperkuat. Pembentukan Komite Stabilitas Sistem Keuangan (KSSK) yang anggotanya mencakup semua lembaga ini menjadi forum strategis untuk membahas dan memitigasi risiko lintas sektoral dari aset digital (UU No. 9 Tahun 2016).

E. Badan Pengawas Perdagangan Berjangka Komoditi (BAPPEBTI)

Sebagai lembaga yang ditunjuk oleh pemerintah untuk mengawasi perdagangan fisik aset kripto, Bappebti memegang peran sentral dalam melegitimasi sekaligus meregulasi industri ini di Indonesia. Sub-bab ini akan mengupas peran pengawasan Bappebti, upayanya dalam penegakan kepatuhan APU-PPT, mekanisme perlindungan konsumen, serta evaluasi regulasi yang dilakukannya (Bappebti, 2019).

1. Peran Pengawasan terhadap Pedagang Fisik Aset Kripto

Peran utama Bappebti adalah menetapkan kerangka regulasi dan melakukan pengawasan terhadap seluruh ekosistem perdagangan fisik aset kripto. Ini mencakup pemberian izin, pengawasan operasional, dan penindakan terhadap Pedagang Fisik Aset Kripto (PFAK), Bursa Berjangka, serta Lembaga Kliring Berjangka (Bappebti, 2019). Bappebti menetapkan syarat-syarat ketat yang harus dipenuhi oleh sebuah perusahaan untuk dapat menjadi PFAK, termasuk modal minimum, infrastruktur teknologi yang andal, dan standar keamanan siber.

Pengawasan Bappebti bertujuan untuk memastikan bahwa perdagangan aset kripto berjalan secara teratur, wajar, dan efisien. Lembaga ini berwenang untuk melakukan audit dan pemeriksaan terhadap PFAK untuk memastikan mereka mematuhi semua peraturan yang berlaku. Bappebti juga yang menentukan daftar aset kripto yang legal untuk diperdagangkan di Indonesia, melalui proses evaluasi risiko dan utilitas dari setiap koin atau token (Bappebti, 2020).

Dengan adanya pengawasan ini, Bappebti berusaha memberikan lapisan legitimasi dan keamanan bagi masyarakat yang ingin berinvestasi di aset kripto. Peran ini menempatkan Bappebti sebagai "wasit" di pasar, yang bertugas memastikan semua pemain mengikuti aturan dan menjaga agar pasar tidak berubah menjadi arena penipuan massal (Bappebti, 2019).

2. Penegakan Kepatuhan APU-PPT

Salah satu peran terpenting Bappebti adalah memastikan bahwa PFAK mematuhi rezim Anti-Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU-PPT). Bappebti mewajibkan semua PFAK untuk mendaftar

sebagai Pihak Pelapor ke PPATK dan menerapkan prinsip-prinsip Mengenali Pengguna Jasa (*Know Your Customer* - KYC) (Peraturan Bappebti No. 8 Tahun 2021). Ini berarti setiap nasabah yang membuka akun di PFAK harus melalui proses verifikasi identitas yang ketat, termasuk menyerahkan dokumen identitas dan melakukan verifikasi biometrik.

Bappebti secara aktif mengawasi implementasi program APU-PPT di setiap PFAK. Mereka memeriksa apakah PFAK memiliki sistem pemantauan transaksi yang memadai untuk mendeteksi aktivitas mencurigakan dan apakah mereka secara rutin melaporkan Transaksi Keuangan Mencurigakan (TKM) kepada PPATK. Kegagalan dalam mematuhi kewajiban ini dapat berujung pada sanksi administratif yang berat dari Bappebti, mulai dari peringatan tertulis hingga pencabutan izin usaha (Peraturan Bappebti No. 8 Tahun 2021).

Dengan menegakkan kepatuhan APU-PPT, Bappebti berfungsi sebagai benteng pertahanan pertama untuk mencegah masuknya dana ilegal ke dalam sistem keuangan melalui pintu aset kripto. Peran ini sangat krusial untuk menjaga reputasi Indonesia di mata komunitas internasional dan untuk mematuhi standar yang ditetapkan oleh FATF (FATF, 2021).

3. Mekanisme Perlindungan Konsumen/Investor

Selain pengawasan pasar, Bappebti juga memiliki mandat untuk melindungi kepentingan konsumen atau investor aset kripto. Salah satu mekanismenya adalah dengan mewajibkan PFAK untuk menyediakan informasi yang jelas, akurat, dan tidak menyesatkan mengenai risiko investasi aset kripto (Bappebti, 2019). Iklan atau promosi yang menjanjikan keuntungan pasti secara eksplisit dilarang.

Bappebti juga menetapkan aturan mengenai keamanan dana nasabah. PFAK diwajibkan untuk menyimpan mayoritas aset kripto nasabah dalam *cold wallet* (penyimpanan luring) untuk meminimalisir risiko peretasan. Selain itu, Bappebti juga menyediakan saluran pengaduan bagi masyarakat yang merasa dirugikan oleh PFAK, dan dapat memfasilitasi proses mediasi atau menjatuhkan sanksi jika PFAK terbukti melakukan pelanggaran (Bappebti, 2019).

Meskipun demikian, perlindungan konsumen di pasar kripto tetap menjadi tantangan. Volatilitas harga yang ekstrem bukanlah sesuatu yang bisa diatur oleh Bappebti, dan risiko kerugian akibat keputusan investasi yang salah tetap ditanggung sepenuhnya oleh investor. Oleh karena itu, peran Bappebti lebih fokus pada memastikan integritas operasional PFAK dan transparansi informasi, bukan menjamin keuntungan investor.

4. Evaluasi dan Penyempurnaan Regulasi secara Berkala

Industri aset kripto berkembang dengan sangat dinamis, sehingga regulasi yang statis akan cepat menjadi usang. Menyadari hal ini, Bappebti secara berkala melakukan evaluasi dan penyempurnaan terhadap kerangka regulasinya. Contohnya adalah pembaruan daftar aset kripto yang legal diperdagangkan, serta penyesuaian peraturan untuk mengakomodasi inovasi produk baru sambil tetap memitigasi risikonya (Bappebti, 2020; Peraturan Bappebti No. 8 Tahun 2021).

Proses evaluasi ini melibatkan dialog dengan para pemangku kepentingan, termasuk asosiasi pedagang aset kripto, komunitas investor, serta lembaga penegak hukum dan regulator lainnya seperti PPATK dan BI. Masukan dari berbagai pihak ini penting untuk memastikan bahwa regulasi yang dibuat tidak hanya efektif dalam memitigasi risiko, tetapi juga tidak mematikan inovasi di industri. Fleksibilitas dan kemampuan untuk beradaptasi adalah kunci bagi regulator di era digital.

Ke depan, tantangan besar bagi Bappebti adalah bagaimana mengatur fenomena baru seperti DeFi, NFT (*Non-Fungible Token*), dan produk-produk derivatif kripto yang semakin kompleks. Bappebti harus terus proaktif dalam mempelajari tren global, melakukan studi komparatif dengan regulator di negara lain, dan menyiapkan kerangka regulasi yang antisipatif. Dengan demikian, Bappebti dapat terus menjalankan mandatnya untuk menciptakan ekosistem perdagangan aset kripto yang teratur, adil, dan aman di Indonesia.

Analisis Mendalam Konsep Kunci Bab 10: Ekosistem Kelembagaan Penegakan Hukum

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk menunjukkan bahwa penanggulangan kejahatan kripto bukanlah tugas satu lembaga tunggal, melainkan sebuah upaya kolektif dari sebuah ekosistem yang kompleks. Tujuannya adalah untuk:

1. Memetakan Aktor dan Peran: Mengidentifikasi semua lembaga kunci dan mendefinisikan peran spesifik mereka dalam siklus penegakan hukum (dari pencegahan, intelijen, penyelidikan, penuntutan, hingga regulasi).
2. Menganalisis Alur Kerja: Menggambarkan bagaimana lembaga-lembaga ini berinteraksi dan berkolaborasi dalam menangani sebuah kasus. Misalnya, bagaimana informasi dari PPATK digunakan oleh Polri.
3. Mengidentifikasi Tantangan Spesifik Lembaga: Menyoroti kesulitan-kesulitan unik yang dihadapi oleh setiap lembaga sesuai dengan tugas dan fungsinya.
4. Menyoroti Kebutuhan Sinergi: Menekankan bahwa efektivitas penanggulangan sangat bergantung pada kualitas koordinasi dan sinergi antar lembaga dalam ekosistem tersebut.

Ini adalah analisis "siapa melakukan apa" dalam perang melawan kejahatan ekonomi digital.

Elemen-Elemen Kunci dalam Analisis Ekosistem:

1. Fungsi Utama: Apa tugas pokok lembaga tersebut dalam konteks kejahatan kripto?
2. Kewenangan Hukum: Dari mana lembaga tersebut mendapatkan mandatnya?
3. Tantangan Praktis: Apa hambatan utama yang mereka hadapi di lapangan?
4. Titik Interaksi (Kolaborasi): Dengan lembaga mana saja mereka harus bekerja sama?

Analisis Komparatif: Peran dan Fungsi dalam Ekosistem Kelembagaan

Tabel berikut membedah peran setiap lembaga kunci dalam ekosistem penanggulangan kejahatan *cryptocurrency* di Indonesia.

Lembaga	Fungsi Utama dalam Siklus Penegakan Hukum	Kewenangan Kunci	Tantangan Spesifik	Titik Interaksi Utama (Kolaborasi)
Polri (Dittipidsiber)	Penyelidikan & Penyidikan. Ujung tombak di lapangan. Mengumpulkan bukti, menangkap pelaku.	Melakukan patroli siber, penyelidikan, penyitaan barang bukti, dan penangkapan tersangka.	Atribusi Pelaku: Sulitnya mengidentifikasi pelaku anonim. Kerjasama Internasional: Lambatnya proses MLA untuk kasus lintas batas.	PPATK (menerima hasil analisis), Kejaksaan (menyerahkan berkas perkara), Kominfo (memblokir situs).
Kejaksaan Agung	Penuntutan. Membawa kasus ke pengadilan dan membuktikan kesalahan terdakwa.	Merumuskan dakwaan, menyajikan alat bukti di persidangan, menuntut hukuman, dan mengeksekusi putusan.	Kompleksitas Pembuktian: Menjelaskan bukti teknis yang rumit kepada hakim. Menuntut Perampasan Aset: Kesulitan dalam mengeksekusi perampasan aset digital.	Polri (menerima berkas perkara/P-21), Pengadilan (proses persidangan), Lembaga Sitaan (pengelolaan aset).
PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan)	Intelijen Keuangan (Pencegahan & Dukungan Penyidikan). "Mata-mata" di sistem keuangan.	Menerima & menganalisis Laporan Transaksi Keuangan Mencurigakan (LTKM). Membekukan transaksi sementara.	Transaksi Terdesentralisasi (DeFi): Sulitnya memantau transaksi yang tidak melalui PJK/VASP. Analisis Lintas Rantai (*Cross-chain*).	PFAK/Bursa Kripto (menerima laporan), Polri/Kejaksaan/BNN (menyerahkan hasil analisis), FIU negara lain (Egmont Group).

Lembaga	Fungsi Utama dalam Siklus Penegakan Hukum	Kewenangan Kunci	Tantangan Spesifik	Titik Interaksi Utama (Kolaborasi)
OJK & Bank Indonesia	Penjaga Stabilitas Sistem Keuangan (Makroprudensial). Fokus pada pencegahan risiko di sektor formal.	Melarang LJK memfasilitasi kripto. Mengawasi paparan risiko di perbankan. Mengembangkan Rupiah Digital (CBDC).	Risiko Bayangan (*Shadow Banking*): Aktivitas kripto terjadi di luar jangkauan pengawasan langsung mereka. Menjaga Keseimbangan: Antara inovasi dan stabilitas.	BAPPEBTI & KSSK (koordinasi kebijakan), Pemerintah (pengembangan CBDC).
BAPPEBTI	Regulator Industri (Mikroprudensial). Mengawasi pelaku usaha pasar fisik aset kripto.	Memberikan izin, menetapkan aturan main bagi PFAK, menegakkan kepatuhan APU-PPT, dan melindungi konsumen.	Laju Inovasi: Regulasi sering tertinggal dari perkembangan teknologi. Pengawasan Efektif: Terbatasnya sumber daya untuk mengawasi ratusan PFAK.	PPATK (kewajiban pelaporan APU-PPT), ASPAKRINDO (asosiasi industri), OJK/BI (koordinasi kebijakan).

Kontribusi Konsep Ekosistem Kelembagaan dalam Bab 10:

Konsep ini memberikan perspektif holistik dan praktis tentang bagaimana negara bekerja.

1. Menunjukkan Realitas di Lapangan: Bab ini menjelaskan bahwa penegakan hukum bukanlah proses linear yang sederhana, melainkan sebuah jaringan kerja sama yang rumit. Keberhasilan menangkap satu pelaku sering kali merupakan hasil kerja senyap dari beberapa lembaga.
2. Mengidentifikasi Titik Lemah Sistemik: Dengan memetakan interaksi, bab ini dapat menyoroti di mana "rantai" kerja sama ini paling lemah. Apakah pada pertukaran informasi antara PPATK dan Polri? Atau pada koordinasi kebijakan antara Bappebti dan OJK?
3. Menjadi Dasar Rekomendasi Kelembagaan: Analisis tantangan yang dihadapi setiap lembaga secara langsung mengarah pada rekomendasi konkret di Bab 14. Misalnya, tantangan "kapasitas penyidik" di Polri mengarah pada rekomendasi "peningkatan anggaran dan pelatihan". Tantangan "koordinasi" mengarah pada rekomendasi "pembentukan Satgas Nasional".
4. Melengkapi Analisis Hukum: Jika bab-bab sebelumnya fokus pada "perangkat lunak" (aturan hukum), maka Bab 10 fokus pada "perangkat keras" (lembaga yang menjalankan aturan). Sebuah sistem hukum hanya akan efektif jika kedua perangkat ini bekerja dengan baik.

Secara ringkas, Bab 10 membawa pembaca keluar dari ruang sidang dan perpustakaan hukum, lalu masuk ke dalam "ruang rapat" dan "ruang operasi" lembaga-lembaga negara. Ia menunjukkan bahwa perang melawan kejahatan digital adalah perang yang membutuhkan "pasukan gabungan", di mana setiap unit memiliki peran, kekuatan, dan kelemahan yang harus dipahami untuk dapat merancang strategi kemenangan yang efektif.

BAB 11

Strategi Penanggulangan Preventif (Pencegahan)

Setelah membahas modus operandi, analisis hukum, dan peran kelembagaan, fokus buku ini beralih ke horizon masa depan: bagaimana kita dapat mencegah kejahatan ini terjadi sejak awal? Penanggulangan kejahatan yang paling efektif bukanlah penindakan yang keras, melainkan pencegahan yang cerdas dan berlapis. Bab 11 ini secara khusus dirancang untuk membangun sebuah arsitektur strategi preventif yang holistik. *Research gap* yang hendak diisi adalah fragmentasi dalam diskusi mengenai pencegahan, yang sering kali hanya berfokus pada satu aspek (misalnya, regulasi saja atau teknologi saja). Bab ini bertujuan untuk mensintesiskan berbagai pendekatan—sosial-edukatif, regulatori, teknologis, diplomatik, dan moral-etis—ke dalam satu kerangka kerja yang koheren. Pertanyaan penelitian utama yang akan dijawab adalah: Apa saja pilar-pilar strategi preventif yang paling fundamental untuk menanggulangi kejahatan ekonomi digital di Indonesia, dan bagaimana setiap pilar tersebut dapat diimplementasikan secara efektif dengan mengintegrasikan nilai-nilai syariah?

A. Edukasi dan Literasi Digital Syariah

Benteng pertahanan pertama dan terpenting dalam melawan kejahatan ekonomi digital adalah masyarakat yang teredukasi. Tanpa pemahaman yang memadai, masyarakat akan selalu menjadi target empuk bagi para penipu. Sub-bab ini akan membahas strategi pembangunan literasi digital syariah melalui berbagai saluran, mulai dari pendidikan formal hingga peran organisasi keagamaan dan pemanfaatan media modern.

1. Peran Lembaga Pendidikan (Sekolah, Universitas)

Lembaga pendidikan formal memiliki peran strategis dalam menanamkan literasi digital dan keuangan sejak dini. Kurikulum di tingkat sekolah menengah dapat diintegrasikan dengan materi dasar mengenai keamanan siber, cara kerja sistem keuangan digital, dan ciri-ciri investasi bodong. Pengenalan konsep-konsep ini sejak usia sekolah akan membangun generasi yang lebih waspada dan tidak mudah tergiur oleh iming-iming keuntungan instan (OJK, 2022).

Di tingkat perguruan tinggi, perannya menjadi lebih mendalam. Fakultas Ekonomi dan Bisnis Islam harus memasukkan mata kuliah khusus

tentang *fintech*, aset digital, dan ekonomi syariah kontemporer yang secara kritis membahas fenomena *cryptocurrency* (Saeed, 2016). Fakultas Hukum dapat mengembangkan konsentrasi hukum siber yang membahas aspek regulasi dan penegakan hukumnya. Sementara itu, fakultas teknik atau ilmu komputer dapat mendorong riset dan pengembangan teknologi *blockchain* yang aman dan beretika. Kolaborasi riset interdisipliner antar fakultas akan menghasilkan pemahaman yang lebih holistik dan solusi inovatif.

Universitas juga memiliki tanggung jawab pengabdian kepada masyarakat. Melalui program seperti Kuliah Kerja Nyata (KKN) atau seminar publik, mahasiswa dan dosen dapat menjadi agen literasi di komunitas mereka masing-masing. Dengan demikian, lembaga pendidikan tidak hanya mencetak profesional, tetapi juga membangun kesadaran kolektif di tengah masyarakat (Kemendikbudristek, 2021).

2. Peran Organisasi Masyarakat Islam (MUI, NU, Muhammadiyah)

Organisasi masyarakat (ormas) Islam seperti Majelis Ulama Indonesia (MUI), Nahdlatul Ulama (NU), dan Muhammadiyah memiliki jangkauan yang sangat luas hingga ke akar rumput dan memegang otoritas moral yang kuat. Peran mereka dalam menyebarkan literasi digital syariah sangatlah krusial. MUI, melalui komisi fatwanya, telah memberikan panduan awal mengenai hukum *cryptocurrency*, dan panduan ini perlu disosialisasikan secara masif (MUI, 2021).

Lembaga Bahtsul Masail NU dan Majelis Tarjih Muhammadiyah dapat menyelenggarakan kajian-kajian mendalam yang membahas aspek fikih dari berbagai produk *fintech* dan aset digital. Hasil dari kajian ini kemudian dapat disebarluaskan melalui jaringan dakwah mereka, mulai dari khotbah Jumat, pengajian rutin, hingga buletin dan majalah internal. Para dai dan penceramah perlu dibekali dengan materi yang memadai agar dapat menyampaikan pesan kewaspadaan terhadap investasi ilegal dengan bahasa yang mudah dipahami oleh umat.

Selain itu, ormas Islam dapat mendirikan lembaga-lembaga konsultasi atau "klinik" keuangan syariah di tingkat lokal. Lembaga ini dapat menjadi tempat bagi masyarakat untuk bertanya dan memverifikasi legalitas sebuah tawaran investasi sebelum mereka terlanjur menanamkan dananya. Dengan

memanfaatkan struktur organisasi yang sudah mapan, ormas Islam dapat menjadi garda terdepan dalam melindungi umat dari jerat kejahatan ekonomi digital.

3. Materi Edukasi: Risiko, Modus Penipuan, dan Prinsip Syariah

Materi edukasi yang disampaikan harus komprehensif dan relevan. Pertama, materi harus mencakup pemahaman dasar mengenai **risiko** inheren dari aset kripto, terutama volatilitas harga yang ekstrem. Masyarakat harus paham bahwa investasi kripto adalah *high-risk, high-return*, dan mereka tidak boleh menginvestasikan dana yang mereka tidak siap untuk kehilangannya (Bappebti, 2019).

Kedua, materi harus secara spesifik membedah berbagai **modus penipuan** yang umum terjadi. Contoh-contoh nyata dari skema Ponzi, *rug pull*, *phishing*, dan penipuan *giveaway* perlu ditampilkan agar masyarakat dapat mengenali "bendera merah" (*red flags*) sejak awal (Chainalysis, 2023). Edukasi harus menekankan pada satu prinsip emas: "Jika sesuatu terdengar terlalu bagus untuk menjadi kenyataan, kemungkinan besar itu adalah penipuan."

Ketiga, dan ini yang paling penting dalam konteks literasi syariah, materi harus mengaitkan risiko dan modus penipuan tersebut dengan **prinsip-prinsip syariah**. Masyarakat perlu diedukasi bahwa skema Ponzi adalah haram bukan hanya karena ilegal, tetapi karena mengandung unsur penipuan (*tadlīs*) dan memakan harta secara batil. Perdagangan spekulatif yang berlebihan dilarang karena mengandung unsur judi (*maysir*). Transaksi yang tidak jelas objek dan mekanismenya dilarang karena mengandung unsur ketidakpastian (*gharar*) (Al-Qaradawi, 2001). Dengan membingkai isu ini dalam kerangka moral-religius, pesan yang disampaikan akan lebih mengena dan ditaati.

4. Pemanfaatan Media Sosial untuk Kampanye Kesadaran Publik

Di era digital, medan pertempuran informasi ada di media sosial. Para penipu sangat lihai menggunakan platform seperti Instagram, TikTok, Facebook, dan Telegram untuk menjerat korban. Oleh karena itu, upaya edukasi juga harus agresif di platform yang sama. Lembaga pemerintah, ormas Islam, dan para pegiat literasi harus berkolaborasi untuk membanjiri media sosial dengan konten-konten edukatif yang menarik.

Konten tersebut harus dikemas dalam format yang mudah dicerna oleh audiens muda, seperti video pendek, infografis, atau utas (thread) yang viral. Menggandeng *influencer* keuangan yang memiliki kredibilitas dan etika yang baik untuk menyebarkan pesan-pesan positif juga merupakan strategi yang efektif. Kampanye kesadaran publik ini harus berjalan secara berkelanjutan, bukan hanya sesaat setelah sebuah kasus besar meledak.

Selain itu, perlu ada mekanisme pelaporan yang mudah bagi warganet untuk melaporkan akun-akun atau konten yang diduga mempromosikan penipuan. Bekerja sama dengan perusahaan platform media sosial untuk mempercepat proses peninjauan dan penghapusan (takedown) konten-konten berbahaya adalah bagian penting dari strategi ini. Perang melawan disinformasi finansial di media sosial harus dilakukan dengan senjata dan taktik yang setara.

B. Penguatan Regulasi dan Pengawasan

Edukasi saja tidak cukup jika tidak didukung oleh kerangka regulasi yang kuat dan pengawasan yang efektif. Regulasi berfungsi sebagai pagar pembatas yang mempersulit ruang gerak para pelaku kejahatan. Sub-bab ini akan membahas strategi penguatan regulasi, mulai dari pengetatan identifikasi nasabah hingga harmonisasi antarlembaga.

1. Kewajiban Know-Your-Customer (KYC) yang Ketat

Prinsip Mengenali Pengguna Jasa (*Know Your Customer* - KYC) adalah fondasi dari rezim Anti-Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU-PPT). Kewajiban ini harus diterapkan secara ketat, tanpa kompromi, oleh semua Pedagang Fisik Aset Kripto (PFAK) (Peraturan Bappebti No. 8 Tahun 2021). Proses KYC tidak boleh hanya sebatas pengumpulan KTP, tetapi harus mencakup verifikasi berlapis, seperti verifikasi biometrik (liveness detection) untuk memastikan bahwa orang yang mendaftar adalah orang yang sama dengan yang ada di dokumen.

Regulator perlu menetapkan standar minimum yang seragam untuk proses KYC di seluruh industri. Selain itu, perlu ada kewajiban untuk melakukan *Enhanced Due Diligence* (EDD) terhadap nasabah yang tergolong berisiko tinggi, seperti Pejabat Publik (*Politically Exposed Persons*

- PEPs) atau nasabah yang melakukan transaksi dalam volume yang sangat besar. EDD mencakup upaya untuk memahami sumber kekayaan (*source of wealth*) dan sumber dana (*source of fund*) nasabah.

Penegakan sanksi yang tegas bagi PFAK yang lalai dalam menerapkan KYC juga mutlak diperlukan. Kelalaian dalam KYC bukan hanya pelanggaran administratif, tetapi membuka pintu bagi para kriminal untuk menyalahgunakan platform tersebut. Dengan memastikan bahwa tidak ada akun anonim di bursa terpusat, regulator telah secara signifikan mempersempit ruang gerak pelaku kejahatan.

2. Pengembangan Teknologi Pengawasan (SupTech dan RegTech)

Pengawasan secara manual terhadap jutaan transaksi kripto setiap hari adalah hal yang mustahil. Oleh karena itu, regulator harus berinvestasi dalam pengembangan dan adopsi Teknologi Pengawasan (*Supervisory Technology* - SupTech) dan Teknologi Regulasi (*Regulatory Technology* - RegTech) (Auer & Böhme, 2020). SupTech adalah penggunaan teknologi oleh regulator untuk meningkatkan efektivitas pengawasan, sementara RegTech adalah penggunaan teknologi oleh perusahaan untuk mematuhi regulasi.

Contoh implementasi SupTech adalah regulator (seperti Bappebti atau PPATK) menggunakan *platform* analisis *blockchain* untuk memantau aliran dana antar bursa secara *real-time* dan mengidentifikasi transaksi mencurigakan yang mungkin luput dari laporan PFAK. Regulator juga dapat membangun dasbor pengawasan yang terhubung langsung ke sistem PFAK, memungkinkan pemantauan kepatuhan secara otomatis dan berkelanjutan.

Di sisi PFAK, adopsi RegTech dapat membantu mereka mengotomatisasi proses KYC, melakukan skrining nasabah terhadap daftar teroris atau sanksi secara *real-time*, dan menjalankan algoritma pemantauan transaksi untuk mendeteksi pola-pola pencucian uang. Pemerintah dapat memberikan insentif bagi PFAK yang berinvestasi pada teknologi RegTech yang canggih, karena ini pada akhirnya akan meringankan beban pengawasan regulator.

3. Sertifikasi bagi Penyedia Layanan Aset Kripto

Untuk meningkatkan standar profesionalisme dan etika di industri, perlu dipertimbangkan adanya program sertifikasi wajib bagi para individu dan perusahaan yang menyediakan layanan terkait aset kripto. Sertifikasi ini tidak hanya untuk PFAK, tetapi juga bisa diperluas untuk para penasihat investasi kripto, manajer aset digital, atau bahkan *influencer* keuangan yang membahas kripto.

Program sertifikasi ini dapat dikelola oleh asosiasi industri yang diakui oleh regulator. Materi sertifikasi harus mencakup pemahaman mendalam tentang teknologi *blockchain*, regulasi yang berlaku (termasuk APU-PPT), manajemen risiko, dan kode etik profesi. Lulus ujian sertifikasi akan menjadi syarat bagi seseorang untuk dapat memberikan nasihat atau mengelola dana kripto secara profesional.

Dengan adanya sertifikasi, masyarakat akan memiliki acuan untuk membedakan antara penyedia layanan yang profesional dan kredibel dengan para penipu yang hanya bermodal klaim kosong. Regulator juga dapat lebih mudah menindak para pihak yang menawarkan jasa keuangan kripto tanpa memiliki sertifikasi yang diperlukan, serta mencabut sertifikasi bagi mereka yang terbukti melakukan pelanggaran etika atau hukum.

4. Harmonisasi Regulasi antar Lembaga (BI, OJK, BAPPEBTI, PPATK)

Seperti yang telah dibahas di bab sebelumnya, salah satu tantangan utama adalah potensi tumpang tindih atau adanya celah (*gap*) dalam regulasi karena kewenangan yang terbagi di antara beberapa lembaga. Oleh karena itu, harmonisasi dan koordinasi regulasi adalah strategi preventif yang sangat penting. Komite Stabilitas Sistem Keuangan (KSSK) harus menjadi forum utama untuk menyelaraskan kebijakan terkait aset digital (UU No. 9 Tahun 2016).

Harmonisasi ini mencakup beberapa aspek. Pertama, penyamaan definisi dan taksonomi. Semua lembaga harus menggunakan bahasa yang sama dalam mendefinisikan berbagai jenis aset digital dan aktivitas terkait. Kedua, pembuatan "buku aturan" (*rulebook*) bersama atau setidaknya saling terhubung mengenai APU-PPT, perlindungan konsumen, dan keamanan siber yang berlaku lintas sektor.

Ketiga, pembentukan *joint task force* atau pusat krisis bersama untuk merespons insiden besar, seperti peretasan bursa atau kegagalan proyek *stablecoin* yang memiliki dampak sistemik. Dengan adanya harmonisasi, para pelaku usaha tidak akan bingung dengan aturan yang berbeda-beda, dan para penjahat tidak dapat mengeksploitasi celah di antara yurisdiksi regulator yang berbeda.

C. Peran Teknologi dalam Pencegahan

Teknologi adalah pedang bermata dua: ia dapat digunakan untuk melakukan kejahatan, tetapi juga dapat menjadi alat yang sangat ampuh untuk mencegahnya. Memanfaatkan teknologi secara proaktif adalah kunci untuk selangkah lebih maju dari para penjahat. Sub-bab ini akan mengeksplorasi berbagai teknologi yang dapat dimanfaatkan untuk pencegahan kejahatan kripto.

1. Penggunaan Kecerdasan Buatan (AI) untuk Mendeteksi Anomali Transaksi

Kecerdasan Buatan (AI), khususnya *machine learning*, memiliki potensi luar biasa untuk meningkatkan deteksi transaksi mencurigakan. Model AI dapat dilatih dengan jutaan data transaksi historis untuk mempelajari seperti apa "pola normal" perilaku seorang nasabah. Ketika ada transaksi yang menyimpang secara signifikan dari pola normal tersebut (sebuah anomali), sistem akan secara otomatis menandainya untuk ditinjau lebih lanjut oleh analis manusia (PPATK, 2022).

Misalnya, jika seorang nasabah yang biasanya hanya bertransaksi senilai jutaan rupiah tiba-tiba menerima transfer kripto senilai miliaran rupiah dari alamat yang tidak dikenal, sistem AI akan langsung menganggapnya sebagai anomali. AI juga dapat mendeteksi pola pencucian uang yang lebih canggih, seperti *smurfing* (memecah dana menjadi banyak transaksi kecil) atau penggunaan jaringan alamat perantara yang rumit, yang sulit dideteksi oleh mata manusia.

Penerapan AI tidak hanya meningkatkan akurasi deteksi, tetapi juga efisiensi, karena mengurangi jumlah *false positives* (peringatan palsu) yang harus ditinjau oleh analis. Baik regulator maupun PFAK harus didorong

untuk mengadopsi teknologi ini sebagai bagian standar dari sistem pemantauan mereka.

2. Pengembangan Alat Analisis Blockchain (Blockchain Analytics Tools)

Alat analisis *blockchain* adalah "mikroskop" bagi para penegak hukum dan regulator untuk melihat apa yang terjadi di dalam *blockchain*. Perusahaan seperti Chainalysis, Elliptic, dan TRM Labs telah mengembangkan *platform* canggih yang dapat melacak aliran dana, mengidentifikasi alamat yang terkait dengan aktivitas ilegal (seperti peretasan, pasar gelap, atau pendanaan terorisme), dan memberikan "skor risiko" untuk setiap alamat atau transaksi (Chainalysis, 2023).

Pemerintah Indonesia, melalui lembaga seperti Polri, PPATK, dan Bappebti, harus berinvestasi dalam melisensikan alat-alat ini dan melatih para analisnya untuk menggunakannya secara mahir. Alat ini memungkinkan pelacakan aset curian secara *real-time* dan dapat memberikan bukti digital yang kuat di pengadilan. PFAK juga harus diwajibkan untuk menggunakan alat serupa untuk melakukan skrining terhadap setoran dan penarikan dana kripto dari nasabah mereka.

Selain menggunakan alat komersial, pemerintah juga dapat mendukung pengembangan alat analisis *blockchain open-source* di dalam negeri melalui kerja sama dengan universitas dan komunitas riset. Memiliki kapabilitas analisis *blockchain* yang mandiri adalah aset strategis yang penting untuk kedaulatan digital negara.

3. Peningkatan Keamanan Dompet Digital dan Bursa

Mencegah kejahatan juga berarti memperkuat pertahanan agar tidak mudah dibobol. Regulator harus menetapkan standar keamanan siber minimum yang sangat tinggi bagi PFAK. Standar ini harus mencakup kewajiban untuk menyimpan mayoritas aset nasabah dalam *cold storage* (dompet luring yang tidak terhubung ke internet), yang jauh lebih aman dari serangan peretas (Bappebti, 2019).

Standar tersebut juga harus mewajibkan implementasi fitur-fitur keamanan berlapis bagi pengguna, seperti otentikasi dua faktor (2FA) yang wajib, notifikasi login dari perangkat baru, dan mekanisme *whitelisting*

alamat penarikan. PFAK juga harus secara rutin menjalani audit keamanan oleh pihak ketiga yang independen dan memiliki program *bug bounty* untuk mendorong para peretas etis menemukan dan melaporkan kerentanan sebelum dieksploitasi oleh penjahat.

Di sisi pengguna, edukasi mengenai cara mengamankan dompet digital pribadi (*non-custodial wallet*) juga penting. Pengguna perlu diajarkan tentang pentingnya menjaga kerahasiaan *private key* atau *seed phrase* dan bahaya berinteraksi dengan *smart contract* yang tidak terverifikasi. Keamanan adalah tanggung jawab bersama antara penyedia layanan dan pengguna.

4. Konsep Identitas Digital Terdesentralisasi (Decentralized ID)

Salah satu inovasi teknologi *blockchain* yang paling menjanjikan untuk pencegahan kejahatan adalah Identitas Digital Terdesentralisasi (*Decentralized ID* - DID) atau *Self-Sovereign Identity* (SSI). Konsep ini memungkinkan individu untuk memiliki dan mengontrol identitas digital mereka sendiri tanpa bergantung pada penyedia terpusat seperti pemerintah atau perusahaan teknologi (W3C, 2022). Identitas ini dapat diverifikasi secara kriptografis di *blockchain*.

Dalam praktiknya, seorang pengguna dapat memiliki DID yang berisi "klaim" terverifikasi tentang identitas mereka (misalnya, "berusia di atas 18 tahun," "warga negara Indonesia," "telah lulus KYC di bursa A"). Ketika mereka ingin menggunakan layanan baru, mereka hanya perlu menunjukkan klaim yang relevan tanpa harus menyerahkan seluruh data pribadi mereka. Ini meningkatkan privasi sekaligus memungkinkan kepatuhan terhadap regulasi.

Bagi regulator, DID dapat memecahkan masalah KYC di dunia DeFi. Sebuah protokol DeFi dapat diprogram untuk hanya berinteraksi dengan alamat yang memiliki klaim "telah lulus KYC" yang valid, tanpa perlu mengetahui identitas asli pengguna. Ini akan menciptakan ekosistem DeFi yang patuh terhadap regulasi (*compliant DeFi*) dan mencegah dana ilegal masuk. Pemerintah perlu mulai menjajaki dan membuat purwarupa implementasi DID sebagai infrastruktur identitas digital nasional di masa depan.

D. Kerjasama Internasional

Kejahatan siber tidak mengenal batas negara, maka penanggulangannya pun tidak boleh berhenti di batas negara. Kerja sama internasional yang efektif adalah pilar yang tak terpisahkan dari strategi pencegahan dan penindakan. Sub-bab ini akan membahas berbagai bentuk kerja sama internasional yang perlu diperkuat.

1. Pentingnya Perjanjian Bantuan Hukum Timbal Balik (MLA)

Seperti dibahas sebelumnya, Bantuan Hukum Timbal Balik (MLA) adalah mekanisme formal bagi penegak hukum untuk meminta bukti atau bantuan hukum dari negara lain. Indonesia harus terus secara proaktif memperluas jaringan perjanjian MLA, terutama dengan negara-negara yang menjadi pusat aktivitas kripto atau surga bagi para penjahat siber (Kementerian Hukum dan HAM, 2019).

Selain memperbanyak jumlah perjanjian, penting juga untuk menyederhanakan dan mempercepat proses MLA itu sendiri. Proses birokrasi yang panjang sering kali menjadi penghambat utama. Perlu dijajaki penggunaan platform digital yang aman untuk pertukaran permintaan dan bukti MLA, menggantikan jalur diplomatik konvensional yang lambat.

Indonesia juga harus memastikan bahwa perjanjian MLA yang baru secara eksplisit mencakup aset digital dan bukti elektronik. Ini akan memberikan landasan hukum yang lebih kuat bagi penyidik dan jaksa ketika meminta data terkait transaksi *cryptocurrency* dari otoritas di negara lain.

2. Standar Global dari Financial Action Task Force (FATF)

Financial Action Task Force (FATF) adalah organisasi antarpemerintah yang menetapkan standar global untuk pemberantasan pencucian uang dan pendanaan terorisme. Kepatuhan terhadap rekomendasi FATF sangat penting bagi reputasi dan integrasi sebuah negara ke dalam sistem keuangan global. Indonesia, yang telah menjadi anggota penuh FATF, memiliki kewajiban untuk mengimplementasikan semua rekomendasi FATF, termasuk yang terkait dengan aset virtual (FATF, 2021).

Salah satu rekomendasi terpenting adalah "Travel Rule" (Rekomendasi 16), yang mewajibkan penyedia layanan aset virtual (VASP) untuk saling bertukar informasi mengenai pengirim dan penerima transaksi kripto di atas ambang batas tertentu. Implementasi Travel Rule secara efektif akan membuat transaksi kripto menjadi lebih transparan dan mempersulit pelaku kejahatan untuk memindahkan dana secara anonim antar bursa di yurisdiksi yang berbeda.

Pemerintah Indonesia, melalui Bappebti dan PPATK, harus terus memastikan bahwa regulasi nasional sejalan dengan standar FATF yang terus berkembang. Kepatuhan terhadap standar global ini tidak hanya akan mencegah Indonesia dari masuk daftar abu-abu (*grey list*) FATF, tetapi juga akan memperkuat sistem pertahanan negara terhadap aliran dana ilegal.

3. Berbagi Informasi Intelijen Antar Negara

Di luar mekanisme formal seperti MLA, kerja sama informal dalam berbagi informasi intelijen juga sangat penting. PPATK, melalui keanggotaannya di Egmont Group, dapat secara cepat bertukar informasi intelijen keuangan dengan FIU di negara lain (Egmont Group, 2023). Demikian pula, Dittipidsiber Polri dapat menjalin hubungan langsung dengan unit-unit polisi siber di negara lain melalui jaringan Interpol.

Kerja sama informal ini sering kali lebih cepat dan fleksibel daripada MLA. Misalnya, jika Polri sedang melacak aset curian yang dipindahkan ke bursa di negara lain, mereka dapat segera menghubungi polisi di negara tersebut untuk meminta bantuan "pembekuan sementara" aset tersebut sambil menunggu proses MLA yang formal dimulai.

Untuk meningkatkan efektivitas kerja sama ini, perlu ada penempatan atase kepolisian dan atase hukum di kedutaan-kedutaan besar Indonesia di negara-negara kunci. Para atase ini dapat berfungsi sebagai jembatan komunikasi dan fasilitator kerja sama penegakan hukum sehari-hari.

4. Upaya Ekstradisi Pelaku Kejahatan Lintas Batas

Tujuan akhir dari kerja sama internasional adalah membawa pelaku kejahatan ke pengadilan. Ketika seorang pelaku kejahatan siber yang merugikan warga negara Indonesia berhasil diidentifikasi dan ditemukan berada di negara lain, langkah selanjutnya adalah mengupayakan ekstradisi.

Ekstradisi adalah proses penyerahan seorang tersangka atau terpidana oleh negara tempat ia ditemukan kepada negara yang meminta penyerahan untuk diadili atau menjalani hukuman.

Sama seperti MLA, ekstradisi didasarkan pada perjanjian antarnegara. Indonesia perlu terus memperluas jaringan perjanjian ekstradisinya. Dalam negosiasi perjanjian baru, penting untuk memastikan bahwa kejahatan siber dan kejahatan terkait *cryptocurrency* secara eksplisit tercakup sebagai "kejahatan yang dapat diekstradisikan" (*extraditable offenses*).

Proses ekstradisi sering kali rumit dan politis, tetapi keberhasilan dalam mengekstradisi beberapa buronan kelas kakap akan mengirimkan pesan yang sangat kuat kepada para penjahat siber di seluruh dunia: tidak ada tempat yang aman untuk bersembunyi. Upaya penegakan hukum Indonesia tidak akan berhenti di perbatasan.

E. Pendekatan Moral dan Etika Islam

Strategi pencegahan yang paling mendasar dan berkelanjutan adalah yang dibangun di atas fondasi moral dan etika yang kokoh. Hukum dan teknologi hanya dapat mengatur perilaku dari luar, tetapi etikalah yang membimbing perilaku dari dalam. Sub-bab ini akan membahas bagaimana internalisasi nilai-nilai Islam dapat menjadi benteng pertahanan moral melawan kejahatan ekonomi digital.

1. Internalisasi Nilai Amanah, Jujur (Shiddiq), dan Profesional (Itqan)

Pencegahan kejahatan dimulai dari individu. Para pelaku usaha, pengembang teknologi, dan investor di ekosistem ekonomi digital perlu menginternalisasi nilai-nilai fundamental dalam etika bisnis Islam. Nilai pertama adalah amanah, yaitu kepercayaan dan tanggung jawab. Penyedia layanan yang memegang dana nasabah harus sadar bahwa mereka memegang amanah yang akan dipertanggungjawabkan di hadapan Tuhan. Kesadaran ini akan mencegah mereka dari menyalahgunakan atau melalaikan pengelolaan dana tersebut (Chapra, 2000).

Nilai kedua adalah jujur (*shiddiq*). Kejujuran dalam berpromosi, transparansi dalam menjelaskan risiko, dan keterbukaan mengenai struktur biaya adalah manifestasi dari nilai *shiddiq*. Seorang *influencer*

atau pemasar yang jujur tidak akan pernah mempromosikan produk yang ia tahu berpotensi merugikan pengikutnya, karena ia sadar akan dosa dari kesaksian palsu (Al-Qaradawi, 2001).

Nilai ketiga adalah profesional (*itqan*). *Itqan* berarti melakukan segala sesuatu dengan cara terbaik, teliti, dan profesional. Bagi seorang pengembang, *itqan* berarti menulis kode yang aman dan telah diuji dengan baik. Bagi seorang operator bursa, *itqan* berarti membangun sistem keamanan yang kokoh dan prosedur operasional yang andal. Bekerja dengan standar profesionalisme tertinggi adalah bagian dari ibadah.

2. Konsep Dosa Jariyah dari Memfasilitasi Kejahatan

Salah satu konsep dalam Islam yang sangat relevan untuk pencegahan adalah dosa jariyah, yaitu dosa yang terus mengalir bahkan setelah pelakunya meninggal. Dosa ini timbul dari perbuatan yang dampaknya terus menerus menimbulkan keburukan, seperti mengajarkan atau memfasilitasi kejahatan (Hadis Riwayat Muslim). Konsep ini perlu disosialisasikan secara luas.

Seorang *influencer* yang mempromosikan skema Ponzi harus disadarkan bahwa setiap kali ada orang yang tertipu karena promosinya, sebagian dosa dari penipuan itu akan mengalir kepadanya. Seorang pengembang yang menciptakan *smart contract* untuk perjudian online harus paham bahwa selama kontrak itu digunakan, ia akan terus menanggung dosa dari setiap transaksi perjudian yang terjadi.

Internalisasi konsep dosa jariyah ini dapat menjadi rem moral yang sangat kuat. Ia akan membuat orang berpikir seribu kali sebelum terlibat dalam aktivitas yang berada di "wilayah abu-abu", karena konsekuensi spiritualnya tidak sepadan dengan keuntungan duniawi yang sesaat.

3. Peran Ulama dalam Memberikan Tuntunan Moral

Di tengah kompleksitas dan kecepatan perubahan teknologi, masyarakat membutuhkan figur yang dapat memberikan tuntunan moral yang jernih dan menenangkan. Di sinilah peran para ulama dan cendekiawan Muslim menjadi sangat vital. Ulama tidak hanya bertugas mengeluarkan fatwa halal-haram, tetapi juga memberikan bimbingan etis dan spiritual (*taujih*) (Al-Qaradawi, 1999).

Para ulama perlu proaktif dalam mempelajari perkembangan teknologi keuangan agar dapat memberikan panduan yang relevan dan tidak ketinggalan zaman. Mereka harus mampu menjelaskan prinsip-prinsip syariah dengan bahasa yang dapat dipahami oleh para praktisi teknologi dan investor muda. Dialog yang konstruktif antara ulama dan para teknolog akan menjembatani kesenjangan pemahaman dan menghasilkan inovasi yang sejalan dengan nilai-nilai etika.

Selain itu, ulama juga berperan sebagai teladan (*uswah hasanah*). Dengan menunjukkan gaya hidup yang tidak berorientasi pada materialisme dan keserakahan, mereka dapat menginspirasi masyarakat untuk mencari kekayaan dengan cara yang berkah dan bermartabat, bukan dengan jalan spekulasi dan tipu daya.

4. Membangun Ekosistem Ekonomi Digital yang Beretika

Tujuan akhir dari semua strategi preventif ini adalah untuk membangun sebuah ekosistem ekonomi digital yang tidak hanya canggih dan menguntungkan, tetapi juga adil, transparan, dan beretika. Ini adalah sebuah visi jangka panjang yang memerlukan kerja sama dari semua pihak: pemerintah, regulator, pelaku industri, akademisi, ulama, dan masyarakat luas.

Ekosistem yang beretika adalah ekosistem di mana inovasi teknologi diarahkan untuk menciptakan kemaslahatan nyata, bukan untuk memfasilitasi spekulasi kosong. Ini adalah ekosistem di mana keuntungan finansial tidak menjadi satu-satunya ukuran kesuksesan, tetapi juga diimbangi dengan pertimbangan dampak sosial dan spiritual. Ini adalah ekosistem di mana prinsip "tolong-menolong dalam kebaikan dan takwa" menjadi landasan dari setiap interaksi dan transaksi.

Membangun ekosistem seperti ini bukanlah pekerjaan yang mudah, tetapi bukan pula hal yang mustahil. Dengan mengintegrasikan kearifan dari ajaran Islam dengan kecanggihan teknologi modern, Indonesia memiliki potensi untuk menjadi pelopor dalam pengembangan ekonomi digital yang beretika dan membawa berkah bagi semua.

Analisis Mendalam Konsep Kunci Bab 11: Strategi Pertahanan Berlapis untuk Pencegahan

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk menyajikan sebuah kerangka kerja proaktif dan holistik untuk memitigasi risiko kejahatan *cryptocurrency*. Tujuannya bukan untuk menghukum, melainkan untuk "memvaksinasi" ekosistem. Bab ini berfungsi untuk:

1. Mengubah Paradigma: Menggeser fokus dari "bagaimana menangkap penjahat" menjadi "bagaimana membuat kejahatan lebih sulit terjadi dan masyarakat lebih sulit tertipu".
2. Memetakan Lini Pertahanan: Mengidentifikasi berbagai lini pertahanan yang bisa dibangun, mulai dari level individu, industri, nasional, hingga global.
3. Menawarkan Solusi Konkret: Memberikan rekomendasi tindakan spesifik untuk setiap lapisan pertahanan.
4. Mengintegrasikan Aspek Teknis, Regulasi, dan Moral: Menunjukkan bahwa pencegahan yang efektif adalah sinergi antara edukasi (moral & pengetahuan), regulasi (aturan main), teknologi (alat), dan diplomasi (kerjasama).

Ini adalah cetak biru untuk membangun sebuah benteng pertahanan digital yang kokoh.

Elemen-Elemen Kunci dalam Strategi Pertahanan Berlapis:

1. Lapisan Individu & Masyarakat (Pertahanan Paling Dalam): Membuat calon korban menjadi lebih cerdas dan waspada.
2. Lapisan Industri & Regulasi (Pertahanan Nasional): Membuat sistem menjadi lebih sulit untuk disalahgunakan.
3. Lapisan Teknologi (Pertahanan Teknis): Menggunakan alat untuk mendeteksi dan mencegah aktivitas jahat secara otomatis.
4. Lapisan Internasional (Pertahanan Global): Mempersempit ruang gerak pelaku kejahatan di tingkat global.

Analisis Komparatif: Lapisan-Lapisan Strategi Pencegahan

Tabel berikut membedah setiap lapisan pertahanan, menjelaskan fokus, aktor utama, dan contoh tindakan konkretnya.

Lapisan Pertahanan	Fokus Utama	Aktor Kunci	Contoh Tindakan Konkret	Analogi Pertahanan
Edukasi & Literasi Digital Syariah	Memperkuat Individu. Menciptakan "imunitas" pada masyarakat agar tidak mudah tertipu.	Lembaga Pendidikan, Ormas Islam (MUI, NU, Muhammadiyah), Regulator (OJK), Kominfo.	Kampanye media sosial "Waspada Investasi Bodong", memasukkan kurikulum ekonomi digital di universitas, khutbah Jumat tentang bahaya *gharar* dan *maysir*.	Vaksinasi. Membuat individu kebal terhadap "virus" penipuan.
Penguatan Regulasi & Pengawasan	Memperkuat Sistem Nasional. Membuat "aturan lalu lintas" yang jelas dan sulit dilanggar di dalam negeri.	BAPPEBTI, OJK, BI, DPR (Legislatif).	Kewajiban KYC yang ketat, sertifikasi bagi bursa kripto, harmonisasi regulasi antar lembaga melalui KSSK.	Membangun Tembok & Gerbang Kota. Mengatur siapa yang boleh masuk dan apa yang harus dilakukan di dalam "kota" (ekosistem).
Peran Teknologi dalam Pencegahan	Memperkuat Alat Deteksi. Menggunakan teknologi untuk melawan teknologi.	Pelaku Industri (Bursa Kripto), Perusahaan Analisis *Blockchain*, Penegak Hukum.	Menggunakan AI untuk menandai transaksi mencurigakan, alat analisis *on-chain* untuk melacak dana, audit keamanan *smart contract*.	Memasang CCTV & Alarm. Sistem pengawasan otomatis yang beroperasi 24/7 untuk mendeteksi penyusup.
Kerjasama Internasional	Mempersempit Ruang Gerak Global. Mencegah pelaku melarikan diri ke "surga" yurisdiksi yang longgar.	Kemenkumham, PPATK, Polri (Interpol), Kementerian Luar Negeri.	Implementasi "Travel Rule" dari FATF, percepatan proses MLA, berbagi info intelijen antar FIU (Egmont Group).	Aliansi Militer & Perjanjian Ekstradisi. Memastikan tidak ada tempat aman bagi musuh untuk bersembunyi.

Lapisan Pertahanan	Fokus Utama	Aktor Kunci	Contoh Tindakan Konkret	Analogi Pertahanan
Pendekatan Moral & Etika Islam	Memperkuat Fondasi Batin. Membangun kesadaran internal pada pelaku industri dan pengguna untuk tidak berbuat curang.	Ulama, Dai, Pendidik, Pemimpin Industri.	Internalisasi nilai *amanah* dan *shiddiq* dalam kode etik industri, dakwah tentang dosa jariyah dari memfasilitasi kejahatan.	Membangun Kompas Moral. Memberikan panduan internal bagi setiap individu untuk menavigasi jalan yang benar.

Kontribusi Konsep Pertahanan Berlapis dalam Bab 11:

Konsep ini adalah manifesto pencegahan dari buku ini.

1. Menawarkan Harapan dan Proaktivitas: Setelah bab-bab sebelumnya banyak membahas sisi gelap, bab ini menawarkan solusi yang konstruktif dan proaktif. Ia menunjukkan bahwa kita tidak harus pasif menunggu kejahatan terjadi.
2. Menggarisbawahi Tanggung Jawab Bersama: Konsep ini secara gamblang menunjukkan bahwa pencegahan bukanlah tugas pemerintah atau polisi saja. Ia adalah tanggung jawab bersama yang melibatkan akademisi, ulama, pelaku industri, hingga individu.
3. Mengintegrasikan Seluruh Pembahasan: Bab ini secara cerdas merangkai kembali berbagai elemen yang telah dibahas: prinsip syariah (dari Bab 3 & 5), peran regulator (dari Bab 10), dan tantangan global (dari Bab 4).
4. Menjadi Landasan bagi Rekomendasi Akhir: Hampir semua rekomendasi preventif yang akan dirangkum di Bab 14 berasal dari kerangka kerja yang dibangun di Bab 11 ini.

Secara ringkas, Bab 11 berargumen bahwa cara terbaik untuk memenangkan perang melawan kejahatan digital adalah dengan tidak berperang sama sekali—yaitu dengan membangun sistem pertahanan yang begitu kuat dan berlapis sehingga potensi serangan dapat diminimalkan sejak awal. Ini adalah pergeseran dari pemikiran reaktif ke pemikiran strategis dan preventif.

BAB 12

Strategi Penanggulangan Represif (Penindakan)

Meskipun strategi preventif adalah garda terdepan, sebuah sistem penanggulangan kejahatan tidak akan lengkap tanpa strategi represif yang andal dan kredibel. Ketika pencegahan gagal dan kejahatan telah terjadi, negara harus menunjukkan kemampuannya untuk menindak pelaku, memulihkan kerugian, dan menegakkan keadilan. Bab 12 ini dirancang untuk membedah komponen-komponen kunci dari strategi penindakan, mulai dari peningkatan kapasitas aparat, teknik perampasan aset, efektivitas sanksi, hingga perlindungan bagi mereka yang paling terdampak, yaitu korban. *Research gap* yang diisi adalah kebutuhan untuk merumuskan strategi penindakan yang terintegrasi dan adaptif terhadap karakteristik unik kejahatan kripto, melampaui sekadar penerapan pasal-pasal hukum konvensional. Pertanyaan penelitian utama yang akan dijawab adalah: Bagaimana strategi penindakan dapat dioptimalkan untuk meningkatkan efektivitas penegakan hukum terhadap kejahatan *cryptocurrency* di Indonesia, dengan tetap menjunjung tinggi prinsip keadilan bagi semua pihak?

A. Peningkatan Kapasitas Aparat Penegak Hukum

Ujung tombak dari setiap strategi represif adalah aparat penegak hukum (APH) yang kompeten. Tanpa penyidik dan jaksa yang mumpuni, hukum secanggih apa pun akan menjadi macan kertas. Sub-bab ini membahas langkah-langkah konkret untuk meningkatkan kapasitas APH dalam menghadapi kejahatan kripto.

1. Pelatihan Khusus tentang Teknologi Blockchain dan Kripto

Peningkatan kapasitas harus dimulai dengan pelatihan yang intensif dan berkelanjutan bagi penyidik Polri dan jaksa. Materi pelatihan tidak bisa lagi hanya sebatas hukum siber secara umum, tetapi harus masuk ke ranah yang sangat spesifik seperti cara kerja berbagai jenis *blockchain*, perbedaan antara koin dan token, analisis transaksi di *block explorer*, serta modus operandi pencucian uang menggunakan DeFi dan *mixer* (Chainalysis, 2023). Pelatihan ini harus bersifat praktis, mencakup studi kasus dan simulasi pelacakan aset.

Pelatihan ini idealnya diselenggarakan secara berkala untuk memastikan pengetahuan APH selalu terbarui seiring dengan perkembangan teknologi.

Kemitraan dengan lembaga pelatihan internasional, perusahaan analisis *blockchain*, atau universitas yang memiliki pusat riset *blockchain* dapat menjadi jalan untuk mendapatkan materi dan instruktur terbaik (Pratama, 2020). Investasi pada sumber daya manusia melalui pelatihan adalah fondasi dari penegakan hukum siber yang efektif.

2. Penyediaan Peralatan Forensik Digital yang Canggih

Pelatihan harus didukung oleh penyediaan peralatan yang memadai. APH perlu dilengkapi dengan perangkat keras dan perangkat lunak forensik digital standar industri. Ini termasuk *workstation* dengan spesifikasi tinggi untuk analisis data, perangkat untuk *imaging* dan akuisisi data dari berbagai perangkat elektronik, serta lisensi untuk *software* forensik komersial terkemuka (Interpol, 2022).

Secara khusus untuk kejahatan kripto, APH wajib memiliki akses berlangganan ke *platform* analisis *blockchain* seperti Chainalysis, Elliptic, atau TRM Labs. Alat-alat ini sangat vital untuk memvisualisasikan aliran dana, mengidentifikasi keterkaitan antar alamat, dan menandai alamat-alamat yang terkait dengan entitas terlarang. Tanpa alat bantu ini, melacak transaksi di tengah jutaan data *blockchain* ibarat mencari jarum di tumpukan jerami.

3. Pembentukan Unit Khusus Kejahatan Kripto

Mengingat tingkat kekhususannya yang tinggi, penanganan kejahatan kripto akan lebih efektif jika ditangani oleh unit khusus. Di tingkat Polri, Dittipidsiber dapat membentuk sub-direktorat atau satuan tugas yang secara eksklusif fokus pada kejahatan yang melibatkan aset virtual. Demikian pula di Kejaksaan Agung, perlu ada kelompok jaksa spesialis yang didedikasikan untuk menuntut kasus-kasus ini (Kejaksaan RI, 2020).

Unit khusus ini akan diisi oleh personel yang telah menerima pelatihan intensif dan memiliki rekam jejak dalam menangani kasus siber. Dengan adanya unit khusus, proses penanganan kasus dari penyelidikan hingga penuntutan dapat berjalan lebih cepat dan terkoordinasi. Unit ini juga akan menjadi pusat keahlian (*center of excellence*) yang dapat memberikan dukungan teknis kepada unit-unit lain dan mengakumulasi pengetahuan dari setiap kasus yang ditangani.

4. Kolaborasi dengan Ahli Teknologi dan Akademisi

APH tidak harus menjadi ahli dalam segala hal. Membangun jaringan kolaborasi yang kuat dengan para ahli di luar institusi adalah strategi yang cerdas. APH dapat secara rutin melibatkan ahli forensik digital independen, analis keamanan siber dari sektor swasta, dan akademisi dari universitas sebagai saksi ahli dalam proses peradilan (Pratama, 2020).

Kolaborasi ini juga bisa bersifat lebih informal, seperti membentuk dewan penasihat teknologi yang terdiri dari para pakar untuk memberikan masukan strategis kepada pimpinan APH. Selain itu, APH dapat bekerja sama dengan universitas untuk mengembangkan program penelitian bersama atau menawarkan program magang bagi mahasiswa berprestasi di bidang IT, yang dapat menjadi jembatan untuk merekrut talenta-talenta baru di masa depan.

B. Optimalisasi Pelacakan dan Perampasan Aset

Tujuan utama penindakan kejahatan ekonomi adalah memulihkan kerugian dan memastikan "kejahatan tidak menghasilkan keuntungan" (*crime doesn't pay*). Hal ini hanya bisa dicapai melalui pelacakan dan perampasan aset yang efektif. Sub-bab ini membahas strategi teknis dan hukum untuk mengoptimalkan perampasan aset kripto.

1. Teknik Pelacakan Aset di Blockchain (On-chain Analysis)

Pelacakan aset kripto adalah inti dari investigasi kejahatan ini. Penyidik harus mahir menggunakan alat analisis *blockchain* untuk melakukan pelacakan *on-chain*. Teknik ini dimulai dari mengidentifikasi alamat kripto korban dan pelaku, kemudian mengikuti jejak aliran dana dari satu alamat ke alamat lainnya, melintasi berbagai *wallet* dan *smart contract* (Chainalysis, 2023).

Tantangan utama adalah ketika dana masuk ke layanan *mixer* atau *privacy coin* yang dirancang untuk mengaburkan jejak. Meskipun sulit, bukan berarti tidak mungkin. Dengan teknik analisis statistik dan heuristik yang canggih, sering kali jejak dana masih dapat diidentifikasi. Kemampuan untuk membaca dan menafsirkan data *blockchain* adalah keterampilan fundamental bagi penyidik kejahatan kripto.

2. Kerjasama dengan Bursa Kripto untuk Pembekuan Aset

Sebagian besar aliran dana ilegal pada akhirnya akan menuju bursa terpusat (PFAK) untuk dicairkan (*cash out*) menjadi uang fiat. Titik ini adalah kesempatan emas bagi penegak hukum. Oleh karena itu, membangun jalur komunikasi yang cepat dan responsif dengan tim kepatuhan (*compliance team*) di semua PFAK, baik di dalam maupun luar negeri, sangatlah krusial (FATF, 2021).

Ketika penyidik berhasil melacak dana curian menuju sebuah alamat deposit di bursa tertentu, mereka harus dapat segera mengirimkan permintaan resmi untuk membekukan akun dan aset terkait. Kecepatan adalah kunci, karena pelaku dapat memindahkan dananya dalam hitungan menit. Mekanisme pembekuan cepat ini harus memiliki landasan hukum yang jelas untuk melindungi PFAK dari tuntutan hukum nasabahnya.

3. Pengembangan Kerangka Hukum untuk Penyitaan Aset Digital

Setelah aset dibekukan, langkah selanjutnya adalah penyitaan resmi. Hukum Acara Pidana (KUHP) dan UU TPPU yang ada perlu ditinjau dan jika perlu diamandemen untuk secara eksplisit mengatur tata cara penyitaan aset digital. Kerangka hukum ini harus menjawab pertanyaan-pertanyaan teknis seperti: Siapa yang berwenang memegang *private key* dari aset sitaan? Bagaimana cara mendokumentasikan penyitaan aset yang bersifat tidak berwujud? (Hallaq, 2009).

Kerangka hukum tersebut juga harus mengatur tentang bagaimana memperlakukan aset kripto yang nilainya sangat fluktuatif selama proses hukum berjalan. Apakah aset tersebut harus segera dilikuidasi menjadi uang fiat, atau disimpan dalam bentuk aslinya? Setiap pilihan memiliki risiko dan konsekuensi hukum yang perlu diatur dengan jelas untuk menghindari sengketa di kemudian hari.

4. Pengelolaan Aset Kripto Sitaan oleh Negara

Setelah aset berhasil disita dan putusan pengadilan telah berkekuatan hukum tetap untuk merampasnya, negara dihadapkan pada masalah baru: bagaimana mengelola aset rampasan tersebut? Untuk ini, perlu dibentuk sebuah lembaga atau unit khusus yang bertugas sebagai pengelola aset rampasan (*asset management office*), seperti yang sudah ada di beberapa negara (Kementerian Keuangan, 2021).

Unit ini, yang bisa berada di bawah Kementerian Keuangan atau Kejaksaan Agung, harus memiliki kapasitas teknis untuk menyimpan aset kripto secara aman dalam *custodial wallet* berstandar institusional. Mereka juga bertugas untuk melelang atau melikuidasi aset tersebut sesuai dengan perintah pengadilan, dan kemudian mengelola hasilnya, baik untuk dikembalikan kepada korban maupun disetorkan ke kas negara. Profesionalisme dalam pengelolaan aset sitaan penting untuk menjaga nilai aset dan akuntabilitas publik.

C. Efektivitas Pemidanaan

Penindakan hukum mencapai puncaknya di ruang sidang melalui proses pemidanaan. Sanksi yang dijatuhkan oleh hakim tidak hanya bertujuan untuk menghukum pelaku, tetapi juga untuk memberikan efek jera dan memenuhi rasa keadilan. Sub-bab ini membahas bagaimana cara meningkatkan efektivitas pemidanaan dalam kasus kejahatan kripto.

1. Penerapan Sanksi Pidana yang Memberi Efek Jera

Untuk kejahatan ekonomi yang didorong oleh motif keuntungan, sanksi pidana harus dirancang untuk membuat kalkulasi untung-rugi pelaku menjadi negatif. Hukuman penjara yang ringan tidak akan memberikan efek jera yang signifikan. Oleh karena itu, jaksa harus berani menuntut hukuman yang berat, dan hakim diharapkan memberikan putusan yang sepadan dengan skala kerugian dan dampak sosial yang ditimbulkan, terutama bagi para otak intelektual dan bandar kejahatan (Chazawi, 2002).

Efek jera (*deterrence*) bekerja dalam dua level: jera spesifik (mencegah pelaku yang sama mengulangi perbuatannya) dan jera umum (memberikan pelajaran kepada masyarakat luas). Putusan yang berat dan diekspos secara luas oleh media akan mengirimkan sinyal yang jelas kepada calon pelaku bahwa negara tidak main-main dalam memberantas kejahatan ekonomi digital.

2. Kombinasi Pidana Penjara, Denda, dan Perampasan Aset

Efektivitas pemidanaan akan maksimal jika sanksi yang diterapkan bersifat kumulatif. Pidana penjara saja tidak cukup jika pelaku masih bisa menikmati hasil kejahatannya setelah bebas. Oleh karena itu, penerapan

Pasal TPPU yang memungkinkan kombinasi pidana penjara, denda yang besar, dan perampasan seluruh aset hasil kejahatan adalah kunci (UU No. 8 Tahun 2010).

Kombinasi ketiga sanksi ini akan memukul pelaku dari semua sisi: kebebasannya dirampas, kekayaannya disita, dan ia masih dibebani denda yang besar. Pendekatan "memiskinkan koruptor" yang sering didengungkan dalam pemberantasan korupsi juga sangat relevan untuk diterapkan pada pelaku kejahatan ekonomi digital skala besar.

3. Penerapan Hukuman Tambahan (misal: Pencabutan Hak Usaha)

Selain pidana pokok (penjara dan denda), KUHP dan berbagai undang-undang khusus juga mengenal adanya pidana tambahan. Dalam kasus kejahatan ekonomi, pidana tambahan ini bisa sangat efektif. Contohnya adalah pencabutan hak-hak tertentu, seperti hak untuk mendirikan atau menjalankan perusahaan di sektor jasa keuangan selama periode waktu tertentu atau bahkan seumur hidup (KUHP, Pasal 10).

Hukuman tambahan ini berfungsi untuk "mensterilkan" pelaku dari ekosistem ekonomi, mencegahnya untuk kembali menyalahgunakan keahliannya untuk menipu masyarakat. Bagi korporasi yang terbukti terlibat dalam kejahatan, sanksi dapat berupa pembubaran perusahaan atau pencabutan izin usaha.

4. Evaluasi Efektivitas Hukuman dalam Menekan Angka Kejahatan

Sistem peradilan pidana harus menjadi sistem yang terus belajar. Perlu ada mekanisme untuk secara berkala mengevaluasi efektivitas dari berbagai jenis sanksi yang telah dijatuhkan. Apakah hukuman yang berat benar-benar berkorelasi dengan penurunan angka kejahatan sejenis? Apakah sanksi alternatif lebih efektif untuk jenis pelaku tertentu?

Evaluasi ini dapat dilakukan melalui penelitian kriminologis dan sosiologis oleh akademisi bekerja sama dengan Mahkamah Agung dan Kementerian Hukum dan HAM. Hasil evaluasi ini dapat menjadi masukan berharga bagi para hakim dalam menyusun pedoman pemidanaan (*sentencing guidelines*) dan bagi legislator dalam merumuskan kebijakan pemidanaan di masa depan.

D. Perlindungan Saksi dan Korban

Sistem peradilan pidana sering kali terlalu fokus pada pelaku dan melupakan korban. Strategi penindakan yang adil dan humanis harus menempatkan perlindungan dan pemulihan hak-hak korban sebagai prioritas. Sub-bab ini membahas berbagai aspek perlindungan bagi saksi dan korban kejahatan kripto.

1. Mekanisme Pelaporan yang Aman bagi Whistleblower

Dalam banyak kasus kejahatan ekonomi terorganisir, informasi kunci sering kali datang dari orang dalam (*whistleblower*). Mereka bisa jadi adalah karyawan perusahaan yang mengetahui adanya penipuan atau mantan anggota sindikat yang ingin bekerja sama dengan penegak hukum. Melindungi identitas dan keselamatan para *whistleblower* ini sangatlah penting (LPSK, 2018).

Lembaga Perlindungan Saksi dan Korban (LPSK) bersama dengan APH perlu mengembangkan saluran pelaporan yang aman dan anonim. Perlindungan tidak hanya mencakup perlindungan fisik dari ancaman, tetapi juga perlindungan hukum dari kemungkinan tuntutan balik (misalnya, gugatan pencemaran nama baik) dari pihak yang dilaporkan. Jaminan keamanan ini akan mendorong lebih banyak orang untuk berani melaporkan kejahatan.

2. Hak Korban atas Restitusi dan Ganti Rugi

Hak paling fundamental bagi korban kejahatan ekonomi adalah pengembalian kerugian yang mereka derita. Mekanisme restitusi (pengembalian aset hasil kejahatan) harus menjadi prioritas utama dalam setiap putusan pengadilan. Hakim harus didorong untuk secara aktif memerintahkan pengembalian aset sitaan kepada para korban yang teridentifikasi (UU No. 31 Tahun 2014).

Dalam kasus di mana aset pelaku tidak mencukupi, perlu dipikirkan mekanisme kompensasi dari negara. Dana kompensasi ini bisa bersumber dari dana hasil lelang aset rampasan negara dari kasus-kasus lain. Meskipun tidak dapat mengganti seluruh kerugian, adanya kompensasi menunjukkan bahwa negara hadir dan peduli terhadap penderitaan warganya.

3. Bantuan Hukum bagi Korban Kejahatan Kripto

Korban penipuan investasi sering kali adalah masyarakat awam yang tidak memiliki sumber daya untuk menyewa pengacara. Akibatnya, mereka kesulitan dalam menempuh jalur hukum untuk menuntut hak-haknya. Oleh karena itu, penyediaan bantuan hukum gratis atau bersubsidi bagi para korban sangatlah penting.

Pemerintah, melalui organisasi bantuan hukum yang terakreditasi, dapat menyediakan layanan konsultasi dan pendampingan hukum bagi para korban. Selain itu, OJK dan Bappebti juga dapat memfasilitasi pengajuan gugatan kolektif (*class action*) oleh sekelompok korban terhadap pelaku, yang biayanya bisa lebih ringan karena ditanggung bersama.

4. Pemulihan Psikologis dan Finansial bagi Korban

Kehilangan seluruh tabungan akibat penipuan dapat menimbulkan trauma psikologis yang mendalam, bahkan memicu depresi atau tindakan bunuh diri. Oleh karena itu, pemulihan korban tidak boleh hanya berhenti pada aspek hukum. Negara dan komunitas perlu menyediakan layanan dukungan psikologis bagi para korban (LPSK, 2018).

Selain itu, program pemulihan finansial juga diperlukan. Ini bisa berupa pelatihan literasi keuangan untuk membantu korban mengelola sisa keuangan mereka dengan lebih baik, atau program pemberdayaan ekonomi untuk membantu mereka memulai kembali usaha atau mencari sumber penghasilan baru. Pendekatan holistik yang memulihkan kondisi psikologis dan finansial korban adalah wujud dari keadilan yang seutuhnya.

E. Penegakan Hukum Berbasis Ta'zir

Sebagai penutup dari strategi represif, penting untuk kembali melihat bagaimana prinsip-prinsip hukum pidana Islam, khususnya konsep *ta'zīr*, dapat memberikan inspirasi bagi sistem peradilan modern. *Ta'zīr* menawarkan kerangka kerja pemidanaan yang fleksibel, berorientasi pada kemaslahatan, dan adil.

1. Fleksibilitas Hakim dalam Menjatuhkan Sanksi yang Adil dan Bermanfaat

Prinsip utama *ta'zīr* adalah fleksibilitasnya. Hakim (*qāḍī*) memiliki kewenangan luas untuk memilih jenis dan kadar hukuman yang paling sesuai dengan karakteristik pelaku dan perbuatannya, mulai dari teguran hingga hukuman mati untuk kejahatan terberat (Audah, 2007). Fleksibilitas ini memungkinkan hakim untuk melakukan personalisasi pemidanaan, menjatuhkan sanksi yang benar-benar adil dan bermanfaat.

Prinsip ini sangat relevan untuk menginspirasi sistem peradilan modern agar tidak terlalu kaku pada ancaman hukuman minimum atau maksimum dalam undang-undang. Hakim harus didorong untuk menggunakan diskresinya secara bijaksana, dengan mempertimbangkan semua faktor yang memberatkan dan meringankan, untuk mencapai keadilan substantif, bukan sekadar keadilan prosedural (Kamali, 2000).

2. Pertimbangan Aspek Kemaslahatan Umum dalam Putusan

Tujuan utama dari hukuman *ta'zīr* adalah untuk mewujudkan kemaslahatan umum (*maṣlaḥah 'āmah*) dan menolak kerusakan (*mafsadah*) (Auda, 2008). Ini berarti, dalam menjatuhkan putusan, pertimbangan hakim tidak hanya terbatas pada kesalahan pelaku, tetapi juga pada dampak putusan tersebut bagi masyarakat luas.

Dalam kasus penipuan massal, misalnya, pertimbangan kemaslahatan umum menuntut agar putusan tidak hanya menghukum pelaku, tetapi juga memprioritaskan pengembalian dana kepada ribuan korban untuk mencegah krisis sosial. Dalam kasus peretasan bursa, pertimbangan kemaslahatan menuntut sanksi yang sangat berat untuk memulihkan kepercayaan publik terhadap sistem keuangan digital. Dengan menempatkan kemaslahatan umum sebagai bintang pemandu, putusan pengadilan akan memiliki dampak sosial yang lebih positif.

3. Kemungkinan Sanksi Alternatif (Kerja Sosial, Pelatihan)

Khazanah sanksi *ta'zīr* tidak terbatas pada penjara dan denda. Ia juga mencakup berbagai sanksi alternatif seperti kerja sosial, pengasingan, atau bahkan perintah untuk mengikuti pelatihan tertentu (Al-Mawardi,

1996). Inspirasi ini sangat relevan untuk memperkaya sistem sanksi dalam hukum positif, terutama untuk pelaku kejahatan yang tidak terlalu berat atau pelaku di bawah umur.

Misalnya, seorang peretas muda yang melakukan kejahatan karena iseng dapat dihukum untuk melakukan kerja sosial dengan mengajar keamanan siber di sekolah-sekolah, atau diwajibkan mengikuti pelatihan etika profesi. Sanksi semacam ini jauh lebih konstruktif dan berorientasi pada perbaikan (*iṣlāḥ*) daripada sekadar memasukkan pelaku ke dalam penjara yang justru bisa menjadi "sekolah kejahatan".

4. Relevansi Prinsip Ta'zir dalam Sistem Peradilan Modern

Pada akhirnya, prinsip-prinsip yang terkandung dalam *ta'zīr* menunjukkan bahwa hukum pidana Islam memiliki kerangka yang sangat relevan dan adaptif untuk menghadapi kejahatan modern. Konsep ini memberikan legitimasi kepada negara (*ulil amri*) untuk membuat undang-undang pidana baru (seperti UU ITE dan UU TPPU) untuk merespons kejahatan-kejahatan yang belum ada di masa lalu (Hallaq, 2009).

Dengan memahami semangat di balik *ta'zīr*—yaitu fleksibilitas, proporsionalitas, orientasi pada kemaslahatan, dan keadilan restoratif—sistem peradilan modern di Indonesia dapat diperkaya. Ini bukan tentang mengganti sistem yang ada, melainkan tentang menginternalisasi nilai-nilai filosofis yang luhur untuk menjadikan penegakan hukum lebih adil, lebih manusiawi, dan lebih efektif dalam mewujudkan ketertiban dan kesejahteraan masyarakat.

Analisis Mendalam Konsep Kunci Bab 12: Optimalisasi Kapasitas Represif

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk menyajikan sebuah kerangka kerja untuk memperkuat sisi penindakan (*repressive*) dari sistem peradilan pidana. Tujuannya bukan hanya tentang "menghukum lebih keras", melainkan tentang "menindak lebih cerdas, lebih cepat, dan lebih adil". Bab ini berfungsi untuk:

1. Mengidentifikasi Titik Lemah Penindakan: Menganalisis di mana saja "kebocoran" atau inefisiensi terjadi dalam proses penegakan hukum, mulai dari penyelidikan hingga pemulihan korban.
2. Menawarkan Solusi Peningkatan Kapasitas: Memberikan rekomendasi konkret untuk memperkuat sumber daya manusia, teknologi, dan kerangka hukum yang digunakan dalam penindakan.
3. Menekankan Pentingnya Pemulihan Aset: Menggeser fokus dari sekadar memenjarakan pelaku menjadi upaya proaktif untuk melacak, menyita, dan mengembalikan aset kepada korban.
4. Mengintegrasikan Perlindungan Korban: Menempatkan perlindungan dan pemulihan hak-hak korban sebagai bagian integral dari proses represif, bukan sebagai renungan.

Ini adalah cetak biru untuk memodernisasi dan mengoptimalkan "mesin" penegakan hukum di era digital.

Elemen-Elemen Kunci dalam Optimalisasi Kapasitas Represif:

1. Kapasitas Sumber Daya Manusia (SDM): Keahlian dan pengetahuan aparat.
2. Kapasitas Teknologi: Peralatan dan perangkat lunak yang digunakan.
3. Kapasitas Hukum & Proses: Efektivitas aturan main dalam penyitaan, pemidanaan, dan perlindungan korban.
4. Kapasitas Filosofis: Prinsip-prinsip keadilan yang mendasari penjatuhan hukuman.

Analisis Komparatif: Area-Area Peningkatan Kapasitas Represif

Tabel berikut membedah area-area utama yang perlu dioptimalkan untuk meningkatkan efektivitas penindakan kejahatan *cryptocurrency*.

Area Optimalisasi	Fokus Utama	Masalah yang Dihadapi Saat Ini	Solusi & Strategi yang Diusulkan	Analogi Peningkatan Kapasitas
Peningkatan Kapasitas Aparat (SDM & Teknologi)	Mempertajam "Penyidik". Membuat aparat lebih pintar dan lebih cepat dari pelaku.	Kurangnya penyidik dengan keahlian forensik digital. Ketergantungan pada alat analisis dari luar. Lambatnya adaptasi terhadap modus baru.	Pelatihan khusus & berkelanjutan tentang *blockchain*. Pengadaan *software* analisis *on-chain*. Pembentukan unit khusus kejahatan kripto. Kolaborasi dengan *white hat hackers*.	Mengirim Pasukan Khusus. Bukan tentara biasa, melainkan unit elit yang dilatih dan diperlengkapi khusus untuk misi di medan digital.
Optimalisasi Pelacakan & Perampasan Aset	Mengejar "Uang". Memastikan kejahatan tidak lagi menguntungkan (*crime doesn't pay*).	Aset kripto mudah dipindahkan lintas batas. Kesulitan teknis dalam menyita dan mengelola aset sitaan (penyimpanan *private key*).	Penguasaan teknik *on-chain analysis*. Kerjasama *real-time* dengan bursa untuk pembekuan. Pembentukan kerangka hukum & lembaga pengelola aset sitaan.	Memblokade Rute Pelarian & Menyita Harta Karun. Tidak hanya menangkap perompak, tapi juga merampas kapal dan hartanya.
Efektivitas Pemidanaan	Memberikan "Pukulan" yang Tepat. Memastikan hukuman memberikan efek jera maksimal dan sepadan.	Sanksi terkadang dianggap terlalu ringan. Fokus hanya pada pidana penjara, kurang pada denda dan perampasan aset.	Penerapan sanksi yang proporsional. Kombinasi maksimal: penjara + denda + perampasan aset. Penerapan hukuman tambahan (pencabutan hak usaha).	Serangan Kombo yang Mematikan. Bukan satu pukulan, tapi kombinasi serangan yang melumpuhkan lawan dari berbagai sisi.

Area Optimalisasi	Fokus Utama	Masalah yang Dihadapi Saat Ini	Solusi & Strategi yang Diusulkan	Analogi Peningkatan Kapasitas
Perlindungan Saksi & Korban	Memulihkan "Korban Perang". Menempatkan korban sebagai subjek utama yang haknya harus dipulihkan.	Korban kesulitan melapor karena takut/ malu. Proses restitusi yang rumit dan tidak pasti. Kurangnya bantuan hukum yang terjangkau.	Mekanisme pelaporan yang aman bagi *whistleblower*. Penyederhanaan proses restitusi dalam KUHAP. Penguatan peran LPSK.	Tim Medis & Bantuan Kemanusiaan. Memastikan warga sipil (korban) yang terdampak perang mendapatkan perawatan dan kompensasi.
Penegakan Hukum Berbasis Ta'zir	Mengadopsi "Kearifan" dalam Menghukum. Menerapkan prinsip keadilan yang lebih substantif dan fleksibel.	Sistem peradilan terkadang terlalu kaku dan positivistik, kurang mempertimbangkan kemaslahatan yang lebih luas.	Memberikan ruang diskresi bagi hakim untuk memilih sanksi yang paling bermanfaat. Memprioritaskan *maslahah 'ammah* (misal: restitusi ke ribuan korban > perampasan untuk negara).	Kebijaksanaan Seorang Jenderal. Tidak hanya menghancurkan musuh, tapi juga memikirkan bagaimana cara terbaik untuk memulihkan kedamaian dan ketertiban setelah perang usai.

Kontribusi Konsep Optimalisasi Represif dalam Bab 12:

Konsep ini adalah pelengkap wajib bagi strategi pencegahan di Bab 11.

1. Menyediakan Rencana Cadangan: Bab ini mengakui bahwa tidak ada pertahanan yang sempurna. Ketika pencegahan gagal, negara harus memiliki mekanisme penindakan yang kuat dan efisien.
2. Fokus pada Solusi Praktis: Berbeda dengan bab-bab yang lebih teoretis, bab ini sangat berorientasi pada solusi praktis dan teknis: pelatihan apa yang dibutuhkan, *software* apa yang harus dibeli, bagaimana mengelola aset sitaan.
3. Mengadvokasi Keadilan bagi Korban: Salah satu kontribusi terpenting bab ini adalah mendorong paradigma di mana keberhasilan penegakan hukum tidak hanya diukur dari berapa banyak pelaku yang dipenjara, tetapi juga dari berapa banyak kerugian korban yang berhasil dipulihkan.
4. Menghubungkan Kembali ke Hukum Islam: Sub-bab terakhir secara elegan menghubungkan kembali semua solusi praktis ini ke prinsip filosofis *Ta'zir*, menunjukkan bahwa modernisasi penegakan hukum sangat sejalan dengan semangat fleksibilitas dan kemaslahatan dalam fikih jinayah.

Secara ringkas, Bab 12 adalah manual untuk "memodernisasi angkatan bersenjata" dalam perang melawan kejahatan digital. Ia berargumen bahwa memiliki undang-undang yang bagus tidaklah cukup; negara juga harus berinvestasi secara masif pada orang, teknologi, dan proses yang menjalankan undang-undang tersebut, sambil tetap memegang teguh prinsip keadilan bagi korban.

BAB 13

Masa Depan Regulasi, Inovasi, dan Peran Hukum Islam

Setelah menelusuri sejarah, menganalisis kejahatan, dan merumuskan strategi penanggulangan, buku ini tiba pada babak akhirnya: sebuah pandangan ke masa depan. Dunia digital tidak pernah statis; inovasi hari ini akan menjadi usang esok hari. Oleh karena itu, setiap pembahasan akan menjadi tidak lengkap tanpa adanya proyeksi dan antisipasi terhadap apa yang akan datang. Bab 13 ini bertujuan untuk memetakan tren-tren utama yang akan membentuk masa depan ekonomi digital, menganalisis potensi dan tantangannya, serta merumuskan peran strategis yang dapat diambil oleh Indonesia, baik dari perspektif hukum positif maupun hukum Islam. *Research gap* yang diisi adalah kebutuhan akan sebuah sintesis yang bersifat futuristik, yang tidak hanya merespons masalah saat ini tetapi juga mempersiapkan landasan untuk menghadapi tantangan masa depan seperti CBDC, DeFi Syariah, dan Metaverse. Pertanyaan penelitian utama yang akan dijawab adalah: Bagaimana Indonesia dapat secara proaktif mengarahkan inovasi teknologi, mereformasi regulasi, dan merevitalisasi ijtihad hukum Islam untuk mewujudkan ekosistem ekonomi digital yang maju, adil, dan beretika?

A. Arah Pengembangan Rupiah Digital (Central Bank Digital Currency – CBDC)

Salah satu respons kebijakan paling signifikan terhadap fenomena aset kripto adalah pengembangan mata uang digital oleh bank sentral. Sub-bab ini akan mengkaji Proyek Garuda yang diinisiasi oleh Bank Indonesia, menganalisis potensi dan tantangannya, serta memberikan tinjauan awal dari perspektif fikih muamalah.

1. Konsep dan Desain Proyek Garuda oleh Bank Indonesia

Proyek Garuda adalah inisiatif Bank Indonesia untuk menjajaki desain *Central Bank Digital Currency* (CBDC) bagi Indonesia, yang disebut sebagai Rupiah Digital. Dalam buku putihnya, Bank Indonesia menguraikan desain Rupiah Digital yang akan diterbitkan dalam dua jenis: CBDC ritel untuk penggunaan publik dan CBDC wholesale untuk transaksi antarbank dan lembaga keuangan (Bank Indonesia, 2022). Desain ini direncanakan untuk diimplementasikan secara bertahap, dimulai dari CBDC wholesale, kemudian diperluas ke CBDC ritel.

Rupiah Digital akan menjadi representasi digital dari uang fiat Rupiah, sehingga ia merupakan kewajiban langsung dari Bank Indonesia. Berbeda dengan aset kripto swasta yang nilainya fluktuatif, nilai Rupiah Digital akan setara 1:1 dengan uang kertas Rupiah dan dijamin sepenuhnya oleh negara. Teknologi yang akan digunakan kemungkinan besar adalah *Distributed Ledger Technology* (DLT) atau *blockchain*, namun dalam bentuk yang terpusat dan terkontrol (*permissioned blockchain*), di mana hanya pihak-pihak yang berwenang (BI dan lembaga keuangan yang ditunjuk) yang dapat menjadi validator transaksi (Auer & Böhme, 2020).

2. Potensi CBDC dalam Mengurangi Risiko Kripto Swasta dan Meningkatkan Inklusi Keuangan

Kehadiran Rupiah Digital memiliki potensi besar untuk memitigasi beberapa risiko yang ditimbulkan oleh aset kripto swasta. Sebagai alat pembayaran digital yang aman, stabil nilainya, dan dijamin oleh negara, Rupiah Digital dapat menjadi alternatif yang jauh lebih superior dibandingkan *stablecoin* swasta yang memiliki risiko kegagalan (*de-pegging*) atau aset kripto spekulatif (Bank Indonesia, 2022). Hal ini dapat mengurangi penggunaan kripto swasta untuk tujuan pembayaran dan melindungi masyarakat dari volatilitas yang ekstrem.

Selain itu, Rupiah Digital berpotensi besar untuk meningkatkan inklusi keuangan. Dengan desain yang tepat, masyarakat yang tidak memiliki rekening bank (*unbanked*) dapat memiliki dompet Rupiah Digital hanya dengan menggunakan nomor telepon atau identitas digital, memberikan mereka akses ke ekosistem pembayaran modern. Ini akan mempermudah penyaluran bantuan sosial pemerintah, memfasilitasi transaksi UMKM, dan mengurangi ketergantungan pada uang tunai yang kurang efisien (BIS, 2021).

3. Tantangan Privasi, Keamanan Siber, dan Pengawasan dalam Implementasi CBDC

Di balik potensinya, implementasi CBDC juga menghadirkan tantangan yang signifikan. Tantangan pertama adalah privasi. Karena diterbitkan dan dikontrol oleh bank sentral, setiap transaksi Rupiah Digital berpotensi untuk dilacak dan diawasi. Hal ini menimbulkan kekhawatiran mengenai pengawasan massal (*mass surveillance*) oleh negara dan hilangnya

anonimitas yang dimiliki oleh uang tunai (Auer & Böhme, 2020). Menemukan keseimbangan antara transparansi untuk mencegah kejahatan dan perlindungan privasi individu akan menjadi tantangan desain yang krusial.

Tantangan kedua adalah keamanan siber. Sebagai infrastruktur keuangan inti negara, sistem Rupiah Digital akan menjadi target utama bagi para peretas, baik yang disponsori oleh negara lain maupun sindikat kriminal. Serangan siber yang berhasil melumpuhkan sistem CBDC dapat menyebabkan krisis keuangan nasional. Oleh karena itu, sistem ini harus dibangun dengan standar keamanan tertinggi yang pernah ada (BIS, 2021). Tantangan ketiga adalah dampak pada sistem perbankan. Jika masyarakat berbondong-bondong memindahkan dananya dari simpanan bank ke dompet Rupiah Digital, bank dapat mengalami krisis likuiditas, yang akan mengganggu fungsi intermediasi mereka dalam menyalurkan kredit.

4. Tinjauan Fikih Muamalah terhadap Konsep dan Mekanisme Rupiah Digital

Dari perspektif fikih muamalah, konsep Rupiah Digital pada dasarnya dapat diterima sebagai bentuk modern dari uang (*nuqūd*). Selama ia diterbitkan dan dijamin oleh otoritas yang sah (*ulil amri*, dalam hal ini Bank Indonesia) dan diterima secara luas oleh masyarakat sebagai alat tukar, maka ia memenuhi syarat sebagai uang yang sah secara syar'i (Al-Zuhaili, 2003). Statusnya sebagai kewajiban langsung dari bank sentral membuatnya lebih kuat daripada uang giral yang merupakan kewajiban dari bank komersial.

Namun, beberapa aspek teknis dan kebijakan memerlukan kajian fikih lebih lanjut. Misalnya, jika Rupiah Digital dirancang untuk bisa mendapatkan bunga (remunerasi), maka ini jelas akan masuk ke dalam kategori riba dan haram. Selain itu, isu privasi juga menjadi perhatian fikih. Prinsip *ḥifẓ al-khuṣūṣiyyah* (perlindungan privasi) adalah bagian penting dari syariah, dan pengawasan berlebihan terhadap transaksi individu tanpa landasan hukum yang jelas dapat dianggap sebagai bentuk *tajassus* (memata-matai) yang dilarang (Kamali, 2015). Oleh karena itu, para ulama perlu dilibatkan dalam perancangan kebijakan privasi dan penggunaan data dalam sistem Rupiah Digital.

B. Inovasi Keuangan Syariah Digital (*Islamic Fintech*)

Teknologi *blockchain* tidak hanya membawa risiko, tetapi juga peluang luar biasa bagi industri keuangan syariah. Dengan memanfaatkan karakteristik transparansi, efisiensi, dan otomatisasi dari *blockchain*, keuangan syariah dapat melompat ke era baru. Sub-bab ini akan mengeksplorasi berbagai potensi inovasi *Islamic Fintech* di era Web3.

1. Potensi Tokenisasi Aset Riil Syariah (Sukuk, Properti, Emas) pada Blockchain

Tokenisasi adalah proses mengubah hak atas sebuah aset riil menjadi token digital di *blockchain*. Potensi aplikasi tokenisasi untuk keuangan syariah sangat besar. Bayangkan sebuah proyek properti atau infrastruktur yang dibiayai melalui penerbitan Sukuk. Alih-alih menerbitkan sertifikat kertas, Sukuk tersebut dapat diterbitkan dalam bentuk token digital (*tokenized sukuk*) (Saeed, 2016). Hal ini akan membuat Sukuk menjadi lebih likuid karena dapat diperdagangkan di pasar sekunder secara *peer-to-peer* 24/7 dengan biaya transaksi yang sangat rendah.

Selain Sukuk, aset-aset lain yang sesuai syariah seperti emas, properti sewaan, atau bahkan saham syariah dapat ditokenisasi. Tokenisasi memungkinkan kepemilikan fraksional (*fractional ownership*), di mana investor kecil dapat membeli sebagian kecil dari aset yang mahal, seperti 1/1000 dari sebuah ruko atau 1 gram emas digital. Ini akan secara dramatis meningkatkan aksesibilitas investasi syariah bagi masyarakat luas dan membuka sumber pendanaan baru bagi proyek-proyek produktif (WEF, 2021).

2. Pengembangan Platform Keuangan Terdesentralisasi (DeFi) yang Sesuai Prinsip Syariah

Keuangan Terdesentralisasi (DeFi) saat ini didominasi oleh protokol pinjam-meminjam berbasis bunga yang jelas-jelas haram. Namun, teknologi dasarnya, yaitu *smart contract* yang berjalan secara otonom, dapat direkayasa untuk menciptakan platform DeFi yang sesuai syariah (*Shariah-compliant DeFi*). Alih-alih protokol pinjaman berbunga, dapat dibangun protokol bagi hasil (*profit-sharing*) terdesentralisasi (Schär, 2021).

Misalnya, sebuah *liquidity pool* dapat dirancang berdasarkan akad *Mudharabah*, di mana penyedia likuiditas (*rabb al-māl*) menyetorkan modal, dan protokol (yang dikelola oleh DAO sebagai *muḍārib*) akan menginvestasikan dana tersebut ke dalam strategi investasi yang halal. Keuntungan kemudian akan dibagikan secara otomatis sesuai nisbah yang disepakati di awal. Platform asuransi terdesentralisasi juga dapat dibangun berdasarkan prinsip *Takaful*, di mana para peserta saling menanggung risiko dan menyumbang ke dalam dana *tabarru'*.

3. Peran *Smart Contract* dalam Otomatisasi Akad-akad Syariah (Murabahah, Ijarah, Mudharabah)

Smart contract adalah program komputer yang secara otomatis mengeksekusi ketentuan sebuah perjanjian jika syarat-syarat tertentu terpenuhi. Teknologi ini dapat merevolusi praktik akad-akad syariah dengan membuatnya lebih efisien, transparan, dan bebas dari intervensi manusia yang bisa bias atau lalai. Misalnya, akad jual beli kredit (*Murabahah*) dapat diotomatisasi sepenuhnya (Saeed, 2016).

Bayangkan sebuah *smart contract Murabahah*: nasabah mengajukan pembiayaan untuk membeli barang, lembaga keuangan (LK) membeli barang tersebut dari pemasok, kepemilikan barang secara kriptografis berpindah ke LK, kemudian *smart contract* secara otomatis membuat akad jual beli baru antara LK dan nasabah dengan margin keuntungan yang disepakati, dan kepemilikan berpindah ke nasabah. Seluruh proses yang biasanya memakan waktu berhari-hari dan melibatkan banyak dokumen ini dapat dieksekusi dalam hitungan menit di *blockchain*, dengan jejak audit yang tidak dapat diubah. Hal yang sama dapat diterapkan pada akad sewa (*Ijarah*), bagi hasil (*Mudharabah*), dan lainnya.

4. Tantangan dan Peluang bagi Industri Keuangan Syariah Indonesia di Era Web3

Peluang bagi Indonesia untuk menjadi pemimpin dalam inovasi *Islamic Fintech* sangat besar. Sebagai negara dengan populasi Muslim terbesar dan pasar ekonomi digital yang berkembang pesat, Indonesia memiliki semua bahan baku yang diperlukan. Pengembangan DeFi Syariah dan tokenisasi aset dapat memecahkan masalah inklusi keuangan dan pendanaan infrastruktur secara bersamaan (OJK, 2021).

Namun, tantangannya juga tidak kecil. Pertama, talenta. Industri keuangan syariah kekurangan talenta yang memiliki keahlian ganda, yaitu memahami fikih muamalah secara mendalam sekaligus menguasai teknologi blockchain. Kedua, regulasi. Regulator perlu menciptakan kerangka hukum yang jelas dan mendukung untuk inovasi-inovasi ini, termasuk kejelasan status hukum token aset riil dan platform DeFi. Ketiga, edukasi pasar. Masyarakat dan investor perlu diedukasi mengenai produk-produk baru ini agar mereka dapat memanfaatkannya dengan aman dan bertanggung jawab.

C. Menuju Kerangka Hukum Positif yang Adaptif dan Responsif

Regulasi tidak boleh menjadi penghambat inovasi, tetapi harus berfungsi sebagai pagar pengaman yang mengarahkannya ke jalur yang produktif dan aman. Untuk itu, pendekatan regulasi konvensional yang kaku dan lambat perlu berevolusi. Sub-bab ini membahas strategi untuk menciptakan kerangka hukum yang lebih adaptif dan responsif.

1. Urgensi Pembentukan Undang-Undang Khusus tentang Aset Digital dan Teknologi Blockchain

Saat ini, pengaturan aset digital di Indonesia masih tersebar di berbagai peraturan setingkat peraturan menteri atau lembaga (misalnya, Peraturan Bappebti). Hal ini menciptakan ketidakpastian hukum dan kurangnya landasan yang kokoh. Untuk memberikan kepastian hukum jangka panjang dan mendorong pertumbuhan industri yang sehat, Indonesia memerlukan sebuah Undang-Undang khusus tentang Aset Digital dan Pemanfaatan Teknologi *Blockchain* (UU Aset Digital).

UU ini harus secara komprehensif mendefinisikan berbagai jenis aset digital (mulai dari *cryptocurrency*, *stablecoin*, token utilitas, token sekuritas, hingga NFT), menetapkan hak dan kewajiban para pihak, mengatur penyelenggara layanan, serta memberikan landasan hukum yang jelas untuk penyelesaian sengketa dan penegakan hukum. Kehadiran UU ini akan menjadi sinyal kuat bagi investor global bahwa Indonesia serius dalam mengembangkan ekonomi digitalnya secara bertanggung jawab.

2. Penerapan Prinsip Regulasi Berbasis Teknologi (T*echnology-Neutral Regulation*)

Dalam merancang regulasi untuk inovasi, penting untuk menerapkan prinsip "netral teknologi" (*technology-neutral*). Artinya, regulasi harus fokus pada "apa" aktivitasnya dan "apa" risikonya, bukan pada "bagaimana" teknologi yang digunakannya. Misalnya, jika sebuah entitas menawarkan produk yang esensinya adalah simpan-pinjam dengan imbal hasil, maka ia harus diatur sebagai lembaga jasa keuangan, tidak peduli apakah ia menggunakan aplikasi seluler konvensional atau *smart contract* di *blockchain* (FATF, 2021).

Pendekatan ini mencegah munculnya celah regulasi di mana aktivitas yang sama diperlakukan berbeda hanya karena teknologinya baru. Ini juga membuat regulasi menjadi lebih tahan lama (*future-proof*), karena ia akan tetap relevan meskipun teknologi yang mendasarinya terus berubah. Fokus pada substansi ekonomi dan risiko dari sebuah aktivitas, bukan pada bentuk teknologinya.

3. Pemanfaatan Regulatory Sandbox sebagai Ruang Uji Coba Inovasi yang Aman dan Terkontrol

Untuk inovasi-inovasi baru yang belum jelas model bisnis dan risikonya, regulator tidak harus langsung melarang atau mengizinkannya sepenuhnya. Jalan tengah yang ideal adalah melalui *regulatory sandbox*. Ini adalah sebuah ruang uji coba yang aman dan terkontrol di mana para inovator dapat menguji produk, layanan, atau model bisnis baru mereka pada konsumen dalam skala terbatas, di bawah pengawasan ketat dari regulator (OJK, 2021).

Selama periode *sandbox*, regulator dapat mengamati secara langsung bagaimana produk tersebut bekerja, apa saja risikonya, dan bagaimana konsumen merespons. Berdasarkan hasil pengujian ini, regulator dapat memutuskan apakah produk tersebut layak untuk diizinkan beroperasi secara penuh (dengan seperangkat aturan yang sesuai), perlu dimodifikasi, atau harus dilarang karena terlalu berisiko. *Sandbox* memungkinkan inovasi untuk berkembang tanpa membahayakan stabilitas sistem keuangan atau konsumen secara luas.

4. Mekanisme Revisi Regulasi yang Cepat untuk Mengimbangi Laju Perkembangan Teknologi

Proses legislasi konvensional yang memakan waktu bertahun-tahun untuk mengubah satu undang-undang tidak akan mampu mengimbangi laju perkembangan teknologi digital. Oleh karena itu, perlu ada mekanisme revisi regulasi yang lebih gesit (*agile*). Salah satu pendekatannya adalah dengan membuat undang-undang payung yang bersifat umum dan berbasis prinsip, sementara detail teknisnya diatur dalam peraturan turunan (Peraturan Pemerintah atau Peraturan OJK/BI/Bappebti) yang lebih mudah untuk direvisi.

Selain itu, regulator perlu membentuk unit khusus yang bertugas memantau tren teknologi global dan secara proaktif memberikan rekomendasi untuk pembaruan regulasi. Proses konsultasi publik untuk revisi regulasi juga dapat dipercepat dengan memanfaatkan platform digital. Tujuannya adalah untuk menciptakan siklus umpan balik yang cepat antara perkembangan pasar, identifikasi risiko baru, dan penyesuaian peraturan.

D. Peran Ijtihad Kolektif (Ijtihad Jama'i) dalam Menghadapi Inovasi

Hukum Islam dikenal dengan fleksibilitasnya melalui pintu ijtihad. Namun, menghadapi kompleksitas teknologi modern, ijtihad individual tidak lagi memadai. Diperlukan ijtihad kolektif yang melibatkan berbagai disiplin ilmu. Sub-bab ini membahas peran strategis ijtihad kolektif dalam memberikan panduan syariah di era digital.

1. Pentingnya Forum Dialog antara Ulama Fikih, Ahli Teknologi, Ekonom, dan Regulator

Untuk menghasilkan fatwa atau pandangan hukum Islam yang komprehensif dan akurat mengenai isu-isu seperti DeFi, AI, atau CBDC, para ulama fikih tidak bisa bekerja sendiri. Mereka perlu memahami secara mendalam bagaimana teknologi tersebut bekerja, apa model bisnisnya, dan apa implikasi ekonominya. Oleh karena itu, pembentukan forum dialog multi-disiplin menjadi sebuah keharusan (Auda, 2008).

Forum ini harus secara rutin mempertemukan para ahli fikih muamalah, insinyur *blockchain*, ekonom makro, praktisi industri, dan perwakilan dari regulator (OJK, BI, Bappebti). Dalam forum ini, para teknolog menjelaskan "bagaimana" sesuatu bekerja, para ekonom menjelaskan "apa dampaknya", dan para ulama kemudian menganalisis "apa hukumnya" berdasarkan prinsip-prinsip syariah. Dialog yang saling mencerahkan ini akan mencegah lahirnya fatwa yang prematur atau tidak relevan dengan realitas teknis.

2. Peran Dewan Syariah Nasional (DSN-MUI) dalam Merumuskan Fatwa yang Komprehensif dan Kontekstual

Sebagai lembaga fatwa resmi untuk industri keuangan syariah di Indonesia, Dewan Syariah Nasional-Majelis Ulama Indonesia (DSN-MUI) memegang peran sentral. DSN-MUI perlu terus memperkuat kapasitas internalnya untuk dapat merespons inovasi digital dengan cepat dan cermat. Ini mencakup perekrutan anggota dewan atau tim ahli yang memiliki latar belakang di bidang teknologi dan keuangan modern (MUI, 2021).

Proses penetapan fatwa DSN-MUI harus menjadi puncak dari proses dialog multi-disiplin yang dibahas sebelumnya. Sebelum mengeluarkan fatwa, DSN-MUI harus secara aktif mengundang dan mendengarkan paparan dari para ahli terkait. Fatwa yang dihasilkan haruslah komprehensif, menjelaskan tidak hanya status hukum final (halal/haram), tetapi juga argumentasi (*istinbath*) hukumnya secara rinci, pertimbangan kemaslahatan dan kerusakannya (*maṣāliḥ wa mafāsid*), serta memberikan panduan mitigasi risiko bagi masyarakat.

3. Mengantisipasi Inovasi Masa Depan (seperti Metaverse, AI, Quantum Computing) dan Implikasinya

Ijtihad tidak boleh hanya bersifat reaktif, tetapi juga harus antisipatif. Para ulama dan cendekiawan Muslim perlu mulai mempelajari dan memikirkan implikasi syariah dari teknologi-teknologi yang masih berada di cakrawala, seperti *Metaverse*, Kecerdasan Buatan Generatif (*Generative AI*), dan Komputasi Kuantum (*Quantum Computing*). Misalnya, bagaimana hukum kepemilikan aset virtual di *Metaverse*? Bagaimana status hukum karya seni yang diciptakan sepenuhnya oleh AI? Apa implikasi komputasi kuantum, yang berpotensi memecahkan enkripsi *blockchain* saat ini, terhadap keamanan akad digital?

Dengan memikirkan pertanyaan-pertanyaan ini sejak dini, komunitas hukum Islam dapat mempersiapkan kerangka kerja etis dan normatif sebelum teknologinya diadopsi secara massal. Pendekatan proaktif ini akan memastikan bahwa hukum Islam tidak gagap dan selalu relevan dalam membimbing umat di setiap gelombang perubahan teknologi (Kamali, 2015).

4. Mendorong Lahirnya Fikih Siber (Fiqh al-Cyber) sebagai Disiplin Ilmu Baru

Akumulasi dari berbagai kajian, fatwa, dan riset mengenai isu-isu digital pada akhirnya akan membentuk sebuah disiplin ilmu baru: Fikih Siber (*Fiqh al-Cyber* atau *al-Fiqh al-Raqamī*). Disiplin ini akan secara sistematis membahas hukum-hukum Islam yang berkaitan dengan interaksi manusia di dunia maya, mencakup aspek muamalah (transaksi digital), jinayah (kejahatan siber), munakahat (interaksi sosial online), dan akhlak (etika digital).

Perguruan tinggi Islam perlu didorong untuk membuka program studi atau setidaknya mata kuliah khusus mengenai Fikih Siber. Perlu ditulis buku-buku teks, jurnal-jurnal ilmiah, dan ensiklopedia yang merangkum prinsip-prinsip dan studi kasus dalam disiplin baru ini. Dengan melembagakan Fikih Siber sebagai sebuah disiplin ilmu, proses ijtihad akan menjadi lebih sistematis, terstruktur, dan dapat diwariskan kepada generasi ulama dan cendekiawan berikutnya.

E. Proyeksi Global dan Posisi Strategis Indonesia

Di dunia yang saling terhubung, kebijakan domestik tidak dapat dilepaskan dari tren global. Indonesia harus secara cerdas memposisikan dirinya di tengah persaingan dan kolaborasi internasional. Sub-bab ini akan membahas tren regulasi global dan bagaimana Indonesia dapat mengambil peran strategis.

1. Analisis Tren Regulasi Aset Kripto di Tingkat Global (AS, Uni Eropa, Asia)

Tren regulasi aset kripto di tingkat global menunjukkan pergerakan menuju kejelasan, meskipun dengan pendekatan yang berbeda. Amerika

Serikat mengambil pendekatan berbasis penegakan hukum, di mana SEC secara agresif mengklasifikasikan banyak token sebagai sekuritas. Uni Eropa, di sisi lain, telah meluncurkan kerangka regulasi komprehensif pertama di dunia, yaitu *Markets in Crypto-Assets* (MiCA), yang memberikan kepastian hukum bagi seluruh negara anggotanya (European Parliament, 2023).

Di Asia, Singapura dan Hong Kong berlomba-lomba menjadi pusat kripto dengan mengeluarkan kerangka lisensi yang jelas, sementara Tiongkok mengambil jalur sebaliknya dengan melarang total aktivitas kripto. Indonesia perlu mempelajari berbagai pendekatan ini, mengambil pelajaran dari keberhasilan dan kegagalan negara lain, untuk merumuskan model regulasi yang paling sesuai dengan konteks dan kepentingan nasionalnya.

2. Peluang Indonesia untuk Menjadi Pusat (Hub) Ekonomi dan Keuangan Digital Syariah Dunia

Dengan populasi Muslim terbesar, pasar digital yang masif, dan industri keuangan syariah yang sudah berkembang, Indonesia memiliki peluang emas untuk memposisikan diri sebagai pusat global untuk ekonomi dan keuangan digital syariah. Visi ini dapat diwujudkan dengan menjadi negara pertama yang memiliki ekosistem *Islamic Fintech* berbasis *blockchain* yang paling maju, didukung oleh regulasi yang kondusif dan fatwa-fatwa yang progresif (KNKS, 2019).

Indonesia dapat menjadi tempat lahirnya platform-platform tokenisasi Sukuk global, bursa aset digital syariah, dan protokol DeFi syariah yang digunakan oleh investor dari seluruh dunia. Untuk mencapai ini, pemerintah perlu memberikan insentif bagi para startup *Islamic Fintech*, mempromosikan Indonesia sebagai tujuan investasi di forum-forum internasional, dan secara aktif membentuk standar global untuk keuangan digital syariah.

3. Tantangan Kompetisi Global dan Perlunya Peningkatan Daya Saing Sumber Daya Manusia

Peluang besar selalu datang dengan tantangan yang setara. Negara-negara lain, terutama di kawasan Teluk seperti Uni Emirat Arab dan Arab

Saudi, juga memiliki ambisi yang sama untuk menjadi pusat keuangan digital syariah. Mereka memiliki keunggulan modal yang besar. Oleh karena itu, Indonesia harus bersaing tidak hanya dengan modal, tetapi dengan kualitas sumber daya manusia (SDM).

Peningkatan daya saing SDM adalah kunci. Pemerintah dan industri harus berinvestasi besar-besaran dalam program pendidikan dan pelatihan untuk mencetak lebih banyak *blockchain developer*, ahli keamanan siber, analis data, dan ahli hukum syariah yang paham teknologi. Tanpa pasokan talenta yang memadai, visi Indonesia untuk menjadi pemimpin global akan sulit terwujud.

4. Sinergi antara Kebijakan Nasional dan Standar Internasional untuk Mencegah Arbitrase Regulasi

Di era keuangan tanpa batas, perbedaan regulasi antar negara dapat menciptakan peluang untuk "arbitrase regulasi", di mana perusahaan akan memindahkan operasinya ke negara dengan aturan paling longgar untuk menghindari pengawasan. Hal ini menciptakan perlombaan menuju dasar (*race to the bottom*) yang berbahaya bagi stabilitas keuangan global (FATF, 2021).

Untuk mencegah hal ini, Indonesia harus secara aktif berpartisipasi dalam forum-forum penetapan standar internasional seperti FATF, BIS, dan IOSCO. Kebijakan nasional harus dirancang agar selaras dengan standar-standar global utama, sambil tetap disesuaikan dengan kebutuhan domestik. Sinergi ini penting untuk memastikan bahwa industri aset digital di Indonesia dapat terhubung dengan pasar global secara aman dan bereputasi baik, sekaligus mencegah Indonesia menjadi surga bagi pelaku kejahatan keuangan dari negara lain.

Analisis Mendalam Konsep Kunci Bab 13: Proyeksi Masa Depan dan Visi Strategis

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk memastikan bahwa buku ini tidak hanya relevan untuk hari ini, tetapi juga memberikan panduan untuk menghadapi hari esok. Tujuannya adalah untuk:

1. Mengantisipasi Inovasi: Mengidentifikasi dan menganalisis gelombang inovasi berikutnya (seperti CBDC, DeFi Syariah, Metaverse) sebelum menjadi masalah atau peluang yang masif.
2. Mendorong Regulasi yang Adaptif: Mengadvokasi pergeseran dari regulasi yang reaktif dan kaku menjadi kerangka hukum yang proaktif, adaptif, dan berbasis prinsip.
3. Memperkuat Peran Ijtihad Kolektif: Menekankan bahwa menghadapi masa depan yang kompleks memerlukan kolaborasi intelektual yang erat antara ulama, teknolog, dan regulator.
4. Merumuskan Visi Nasional: Mengartikulasikan sebuah visi besar bagi Indonesia untuk memposisikan diri sebagai pemimpin global dalam ekonomi digital syariah.

Ini adalah bab yang paling visioner, yang mencoba menjawab pertanyaan, "Ke mana arah semua ini, dan bagaimana kita bisa mengendalikannya?"

Elemen-Elemen Kunci dalam Proyeksi Visi Strategis:

1. Analisis Tren Teknologi: Melihat inovasi kunci yang akan membentuk masa depan keuangan.
2. Analisis Tren Regulasi: Mempelajari bagaimana negara-negara lain merespons dan apa yang bisa dipelajari.
3. Analisis Kebutuhan Kelembagaan: Mengidentifikasi mekanisme (seperti *ijtihad jama'i* dan *regulatory sandbox*) yang diperlukan untuk menavigasi masa depan.
4. Positioning Strategis: Menentukan di mana letak keunggulan komparatif Indonesia di panggung global.

Analisis Komparatif: Tren dan Visi Strategis Masa Depan

Tabel berikut membedah berbagai elemen masa depan yang dianalisis dalam Bab 13, menyoroti potensi, tantangan, dan implikasinya.

Tren / Visi	Deskripsi & Tujuan	Potensi & Peluang	Tantangan & Risiko	Implikasi bagi Indonesia
Rupiah Digital (CBDC)	Uang fiat dalam bentuk digital yang diterbitkan dan dijamin oleh Bank Indonesia. Bertujuan untuk efisiensi dan menjaga kedaulatan moneter.	Mengurangi risiko kripto swasta, meningkatkan inklusi keuangan, mempermudah penyaluran bantuan sosial.	Risiko Privasi & Pengawasan: Potensi pengawasan total oleh negara. Risiko Keamanan Siber: Menjadi target peretasan bernilai tinggi.	Langkah Strategis. Harus segera diimplementasikan untuk menjadi tulang punggung ekonomi digital nasional yang sah dan teregulasi.
Inovasi Keuangan Syariah Digital (*Islamic Fintech*)	Menggunakan teknologi *blockchain* untuk menciptakan produk keuangan yang sesuai prinsip syariah.	Tokenisasi Sukuk/Emas: Membuat investasi syariah lebih likuid dan terjangkau. DeFi Syariah: Menciptakan platform *lending* & *staking* tanpa riba. Otomatisasi Akad: *Smart contract* untuk akad *murabahah* atau *ijarah*.	Kompleksitas Fikih: Membutuhkan ijtihad mendalam. Kesiapan SDM: Kurangnya talenta yang menguasai fikih dan teknologi sekaligus.	Peluang Emas. Dengan pasar syariah terbesar, Indonesia bisa menjadi pusat (hub) global untuk inovasi ini.
Kerangka Hukum Adaptif	Pergeseran dari regulasi berbasis aturan yang kaku ke regulasi berbasis prinsip yang fleksibel.	Mendorong Inovasi: Tidak mematikan inovasi baru. Responsif: Dapat menyesuaikan diri dengan cepat terhadap teknologi baru.	Risiko Ketidakpastian Hukum: Regulasi berbasis prinsip bisa multitafsir jika tidak dirumuskan dengan baik.	Urgensi Reformasi. Mendesak untuk segera membentuk UU Aset Digital yang komprehensif dan memanfaatkan Regulatory Sandbox untuk uji coba.

Tren / Visi	Deskripsi & Tujuan	Potensi & Peluang	Tantangan & Risiko	Implikasi bagi Indonesia
Ijtihad Kolektif (Jama'i) & Fikih Siber	Mekanisme di mana ulama, teknolog, ekonom, dan regulator duduk bersama untuk merumuskan fatwa atau panduan.	Fatwa Komprehensif: Menghasilkan panduan yang mempertimbangkan semua aspek (teknis, ekonomi, sosial, syar'i). Responsif & Proaktif: Dapat mengantisipasi masalah sebelum meluas.	Ego Sektoral: Kesulitan menyatukan bahasa dan prioritas dari berbagai disiplin ilmu.	Harus Dilembagakan. Peran DSN-MUI harus diperkuat sebagai fasilitator utama dialog interdisipliner ini untuk melahirkan "Fikih Siber".
Posisi Strategis Global	Visi Indonesia untuk tidak hanya menjadi pasar, tetapi juga pemain utama di panggung ekonomi digital dunia.	Memanfaatkan bonus demografi, pasar digital yang masif, dan status sebagai negara dengan populasi Muslim terbesar.	Kompetisi Global: Persaingan ketat dari negara lain (UEA, Malaysia). Kesenjangan Talenta: Kurangnya SDM unggul di bidang teknologi dan keuangan syariah.	Harus Diraih. Membutuhkan strategi nasional yang terintegrasi antara kebijakan pendidikan, industri, dan diplomasi ekonomi.

Kontribusi Konsep Proyeksi Visi Strategis dalam Bab 13:

Konsep ini adalah puncak dari pemikiran konstruktif dalam buku ini.

1. Berorientasi ke Depan: Bab ini memastikan buku tidak berakhir pada masalah hari ini, tetapi membuka wawasan pembaca tentang apa yang akan datang. Ini memberikan nilai tambah jangka panjang bagi karya tersebut.
2. Menawarkan Peta Jalan (*Roadmap*): Bab ini tidak hanya berteori, tetapi menyajikan sebuah "peta jalan" strategis bagi Indonesia, yang mencakup pengembangan CBDC, penguatan fintech syariah, reformasi regulasi, dan pelembagaan ijtihad.
3. Mengubah Ancaman Menjadi Peluang: Jika bab-bab awal banyak membahas *cryptocurrency* sebagai ancaman, bab ini secara brilian menunjukkan bagaimana teknologi yang sama (*blockchain*) dapat dimanfaatkan untuk menciptakan inovasi keuangan syariah yang luar biasa.
4. Menginspirasi Optimisme: Setelah melalui pembahasan panjang tentang kejahatan dan masalah, bab ini ditutup dengan nada yang optimis dan memberdayakan, memposisikan Indonesia sebagai calon pemimpin, bukan korban, dari disrupsi teknologi.

Secara ringkas, Bab 13 adalah "bab manifesto". Ia mengajak para pemangku kepentingan—pemerintah, ulama, pelaku industri, dan akademisi—untuk berhenti hanya bereaksi terhadap masalah, dan mulai secara proaktif merancang masa depan ekonomi digital yang sesuai dengan nilai-nilai dan cita-cita bangsa. Ini adalah ajakan untuk bertransformasi dari sekadar "pemadam kebakaran" menjadi "arsitek masa depan".

BAB 14

Epilog

Perjalanan panjang buku ini, yang dimulai dari sejarah uang hingga proyeksi masa depan keuangan digital, kini tiba di muaranya. Setelah membedah anatomi *cryptocurrency*, menganalisis modus operandinya dari perspektif hukum positif dan hukum pidana Islam, serta merumuskan strategi penanggulangan yang berlapis, tugas terakhir adalah merajut semua benang merah menjadi sebuah kesimpulan yang padu dan memberikan arah jalan ke depan. Bab 14 ini tidak dimaksudkan sebagai pengulangan, melainkan sebagai sebuah sintesis—distilasi dari argumen-argumen kunci yang telah dibangun di sepanjang buku (Creswell & Creswell, 2018). Bab ini akan menjawab pertanyaan penelitian utama dari keseluruhan buku ini: Bagaimana kerangka hukum pidana Islam dan hukum positif dapat disinergikan untuk menanggulangi kejahatan ekonomi digital berbasis *cryptocurrency* secara efektif seraya membuka jalan bagi inovasi yang bertanggung jawab di Indonesia? Berdasarkan jawaban tersebut, bab ini akan menyajikan serangkaian rekomendasi kebijakan yang terstruktur dan diakhiri dengan sebuah kata penutup yang reflektif.

Rangkuman Temuan Utama (Sintesis)

Dari tiga belas bab pembahasan yang telah dilalui, empat temuan utama mengemuka sebagai pilar-pilar argumen buku ini. Temuan-temuan ini, yang disarikan dari analisis historis, teknologis, yuridis-normatif, dan komparatif, membentuk fondasi bagi rekomendasi dan kesimpulan yang akan ditarik (Soekanto & Mamudji, 2003).

1. Dualisme Sifat Cryptocurrency: Potensi Inovasi dan Risiko Kejahatan

Temuan paling fundamental dari buku ini adalah pengakuan atas sifat dualistik dari *cryptocurrency* dan teknologi *blockchain*. Di satu sisi, teknologi ini menawarkan potensi inovasi yang luar biasa untuk efisiensi, transparansi, dan inklusi keuangan, sebagaimana terlihat dari potensi tokenisasi aset dan DeFi Syariah (Schär, 2021). Teknologi DLT dapat mengurangi biaya intermediasi, mempercepat penyelesaian transaksi, dan menciptakan pasar baru yang lebih mudah diakses oleh masyarakat luas.

Di sisi lain, sifat pseudonim, desentralisasi, dan ketiadaan batasnya telah dieksploitasi secara masif untuk melakukan berbagai kejahatan, mulai dari penipuan, pencucian uang, hingga pendanaan terorisme (Chainalysis, 2023). Mengabaikan salah satu dari dua sisi mata uang ini akan menghasilkan kebijakan yang pincang: regulasi yang terlalu represif akan mematikan inovasi, sementara sikap yang terlalu permisif akan membahayakan stabilitas keuangan dan keamanan publik. Oleh karena itu, pendekatan kebijakan yang seimbang (*balanced approach*) menjadi sebuah keniscayaan.

2. Fleksibilitas Hukum Pidana Islam (melalui Jarimah Ta'zir) dalam Menjangkau Kejahatan Digital Modern

Buku ini secara konsisten menunjukkan bahwa hukum pidana Islam (*fiqh al-jināyah*) memiliki kapasitas dan fleksibilitas yang luar biasa untuk merespons kejahatan-kejahatan modern yang tidak dikenal dalam teks-teks klasik. Melalui pintu *jarīmah ta'zīr*, di mana jenis dan sanksi pidana diserahkan kepada kebijakan penguasa (*ulil amri*) demi kemaslahatan umum, semua modus kejahatan kripto dapat dikualifikasikan sebagai tindak pidana (Audah, 2007). Konsep ini memberikan ruang bagi legislasi baru untuk menghadapi tantangan zaman tanpa harus bertentangan dengan prinsip dasar syariah.

Penipuan investasi dikualifikasikan sebagai *tadlīs* (penipuan) dan *gharar* (ketidakpastian), pencucian uang sebagai *i'ānah 'ala al-ma'ṣiyah* (membantu kejahatan), peretasan sebagai *sariqah ta'zīriyah* (pencurian yang sanksinya ditentukan penguasa), dan pendanaan terorisme sebagai *hirābah* atau *ifsād fil-arḍ* (perusakan di muka bumi) (Kamali, 2000). Ini membantah pandangan bahwa hukum Islam bersifat kaku dan ketinggalan zaman, sebaliknya ia menunjukkan adanya mekanisme internal yang dinamis untuk menjaga relevansinya.

3. Titik Temu dan Harmoni antara Prinsip Hukum Pidana Islam dan Hukum Positif di Indonesia

Analisis komparatif dalam buku ini menemukan adanya titik temu filosofis dan keselarasan praktis yang kuat antara prinsip hukum pidana Islam dan hukum positif di Indonesia. Tujuan perlindungan jiwa, harta, akal, keturunan, dan agama (*Maqāṣid al-Sharī'ah*) selaras dengan tujuan

hukum nasional untuk melindungi segenap tumpah darah Indonesia dan menciptakan ketertiban umum (Auda, 2008). Perlindungan harta (*ḥifẓ al-māl*) dalam Islam paralel dengan perlindungan hak milik dalam konstitusi.

Konsep *ta'zīr* memberikan legitimasi syar'i bagi negara untuk membentuk undang-undang pidana baru seperti UU ITE dan UU TPPU sebagai bentuk kebijakan penguasa untuk mewujudkan kemaslahatan (Hallaq, 2009). Prinsip perampasan harta haram dalam fikih sejalan dengan mekanisme perampasan aset dalam UU TPPU. Harmoni ini menunjukkan bahwa internalisasi nilai-nilai hukum Islam ke dalam pembaharuan hukum nasional bukanlah sebuah utopia, melainkan sebuah kemungkinan yang logis dan dapat diperkaya.

4. Urgensi Pendekatan Holistik: Kombinasi Strategi Preventif, Represif, dan Edukatif

Temuan akhir yang paling krusial adalah bahwa tidak ada satu solusi tunggal untuk menanggulangi masalah yang kompleks ini. Penindakan hukum (represif) yang keras tidak akan efektif jika tidak diimbangi dengan upaya pencegahan (preventif) yang cerdas dan edukasi publik yang masif (LPSK, 2018). Sebuah strategi yang hanya fokus pada penangkapan pelaku tanpa memutus akar masalahnya, yaitu rendahnya literasi dan lemahnya sistem, akan selalu tertinggal.

Buku ini menggarisbawahi bahwa strategi yang holistik harus mencakup lima pilar: (1) Edukasi untuk membangun imunitas masyarakat; (2) Regulasi yang adaptif sebagai pagar pengaman; (3) Teknologi sebagai alat pengawasan; (4) Kerja sama internasional untuk mengatasi sifat lintas batas kejahatan; dan (5) Penguatan etika sebagai fondasi moral (WEF, 2021). Kegagalan pada salah satu pilar akan melemahkan keseluruhan struktur pertahanan, ibarat sebuah bangunan yang fondasinya tidak merata.

Kata Penutup: Menuju Ekosistem Ekonomi Digital yang Aman, Adil, dan Maslahat

Sebagai penutup dari keseluruhan karya ini, beberapa refleksi akhir dan sebuah ajakan perlu disampaikan untuk membingkai masa depan yang akan kita bangun bersama.

1. Refleksi tentang Tanggung Jawab Bersama dalam Mewujudkan Kemaslahatan (Maslahah 'Ammah)

Buku ini telah memaparkan kompleksitas masalah dan serangkaian strategi yang berlapis. Namun, pada akhirnya, semua strategi tersebut akan sia-sia tanpa adanya kesadaran akan tanggung jawab bersama. Mewujudkan ekosistem digital yang membawa kemaslahatan umum (*maṣlaḥah 'āmah*) bukanlah tugas pemerintah semata, bukan pula hanya beban industri atau ulama (Chapra, 2000). Ia adalah sebuah kerja kolektif. Setiap individu, sebagai pengguna, investor, pengembang, atau regulator, memegang sepotong tanggung jawab untuk memastikan bahwa teknologi yang kita ciptakan dan gunakan membawa lebih banyak kebaikan daripada kerusakan.

Tanggung jawab ini adalah manifestasi dari peran kita sebagai khalifah di muka bumi, yang diamanahi untuk mengelola sumber daya (termasuk teknologi) dengan cara yang adil dan tidak merusak. Kesadaran akan akuntabilitas di hadapan Tuhan (*yaum al-hisāb*) harus menjadi kompas moral tertinggi yang membimbing setiap tindakan kita di dunia digital.

2. Visi Masa Depan: Indonesia sebagai Pelopor Ekonomi Digital yang Beretika dan Berkeadilan

Kita berdiri di persimpangan jalan sejarah. Indonesia memiliki semua modal untuk tidak hanya menjadi pasar, tetapi menjadi pemain utama dan pelopor dalam ekonomi digital global. Visi yang harus kita usung bersama adalah menjadikan Indonesia sebagai mercusuar bagi dunia dalam hal pengembangan ekonomi digital yang beretika, berkeadilan, dan berlandaskan pada nilai-nilai luhur (KNKS, 2019). Sebuah ekosistem di mana inovasi teknologi tidak tercerabut dari akar spiritualitasnya, dan kemajuan ekonomi tidak mengorbankan keadilan sosial.

Visi ini bukan angan-angan kosong. Dengan memadukan kekayaan tradisi intelektual Islam dengan semangat inovasi anak bangsa, serta didukung oleh kebijakan yang bijak, Indonesia dapat menunjukkan kepada dunia sebuah model alternatif pengembangan teknologi yang lebih manusiawi dan berkelanjutan.

3. Ajakan untuk Terus Belajar dan Beradaptasi di Tengah Disrupsi Teknologi

Jika ada satu kepastian di era digital, itu adalah ketidakpastian itu sendiri. Teknologi akan terus berubah, melahirkan tantangan dan peluang baru yang hari ini bahkan belum bisa kita bayangkan. Oleh karena itu, sikap yang paling penting untuk dimiliki adalah kerendahan hati untuk terus belajar (*continuous learning*) dan kelincahan untuk terus beradaptasi (*agility*) (Hallaq, 2009). Buku ini bukanlah kata akhir, melainkan sebuah pembuka percakapan—sebuah undangan bagi kita semua untuk tidak pernah berhenti berpikir, berdiskusi, dan berijtihad dalam menghadapi gelombang disrupsi.

Semangat ijtihad, yang merupakan jantung dari dinamisme peradaban Islam, harus kita hidupkan kembali dalam konteks digital. Semangat untuk bertanya, meneliti, berdebat secara konstruktif, dan mencari solusi terbaik bagi umat dan kemanusiaan.

4. Harapan dan Optimisme dalam Menyongsong Era Baru Keuangan Digital

Meskipun buku ini banyak membahas sisi gelap dari inovasi, pesan utamanya bukanlah pesimisme, melainkan optimisme yang waspada. Teknologi pada hakikatnya netral; manusialah yang memberinya warna dan arah. Dengan niat yang lurus, ilmu yang memadai, regulasi yang bijak, dan kolaborasi yang erat, kita memiliki kemampuan untuk mengarahkan kekuatan dahsyat dari teknologi digital ini menuju terwujudnya sebuah tatanan ekonomi yang lebih baik (Chapra, 2000).

Semoga buku ini dapat menjadi salah satu sumbangsih kecil dalam perjalanan besar bangsa Indonesia menyongsong era baru keuangan digital yang aman, adil, dan penuh maslahat. Sebuah era di mana teknologi menjadi alat untuk mendekatkan kita pada keadilan, bukan menjauhkannya.

Analisis Mendalam Konsep Kunci Bab 14: Sintesis, Rekomendasi, dan Refleksi Penutup

Tujuan Fundamental Konsep:

Konsep ini bertujuan untuk memberikan penutupan yang memuaskan dan berdampak bagi pembaca. Tujuannya bukan untuk memperkenalkan informasi baru, melainkan untuk:

1. Mensintesis Temuan: Merangkum argumen-argumen utama dari 13 bab sebelumnya ke dalam beberapa poin kesimpulan yang padat dan mudah diingat.
2. Memberikan Rekomendasi Konkret: Menerjemahkan analisis dan kesimpulan menjadi saran-saran praktis yang ditujukan kepada para pemangku kepentingan spesifik.
3. Mengartikulasikan Visi Akhir: Menyampaikan pesan moral dan filosofis dari buku ini, serta menanamkan rasa urgensi dan optimisme kepada pembaca.
4. Menegaskan Kontribusi Buku: Secara implisit, menunjukkan kontribusi orisinal dari buku ini terhadap khazanah ilmu pengetahuan.

Ini adalah "pidato penutup" yang merangkum semua yang telah dipelajari dan menyerukan tindakan.

Elemen-Elemen Kunci dalam Bab Penutup:

1. Sintesis (Apa yang Telah Kita Pelajari?): Rangkuman temuan-temuan kunci.
2. Rekomendasi (Apa yang Harus Kita Lakukan?): Seruan untuk bertindak (*call to action*) yang terstruktur.
3. Refleksi (Mengapa Ini Semua Penting?): Pesan penutup yang bersifat filosofis dan inspiratif.

Analisis Komparatif: Struktur Bab Penutup

Tabel berikut membedah setiap komponen dari bab terakhir ini, menjelaskan fungsi dan isinya.

Komponen Bab 14	Fungsi Utama	Isi & Argumen Kunci	Target Audiens	Analogi Komponen
Rangkuman Temuan Utama (Sintesis)	Mengingatkan Kembali. Menyaring seluruh isi buku menjadi 4-5 poin inti yang paling krusial.	- Dualisme Kripto: Inovasi vs. Risiko. - Fleksibilitas Fikih: *Jarimah Ta'zir* sebagai solusi. - Harmoni Hukum: Titik temu *Maqashid al-Shari'ah* & Hukum Nasional. - Urgensi Pendekatan Holistik: Preventif + Represif.	Semua Pembaca. Terutama yang ingin mendapatkan intisari buku dengan cepat.	"Abstrak Eksekutif". Ringkasan paling padat dari seluruh laporan.
Rekomendasi untuk Legislatif & Pemerintah	Mendorong Reformasi Struktural. Memberikan masukan kebijakan tingkat tinggi (*high-level policy*).	- Akselerasi RUU Aset Digital. - Penguatan Anggaran & Kapasitas APH. - Pembentukan Satgas Nasional. - Penguatan Diplomasi Internasional.	DPR, Pemerintah (Kemenkeu, Kemenkumham, Kominfo), Pimpinan Lembaga (Polri, PPATK, BI, OJK).	"Nota Kebijakan (Policy Brief)". Saran konkret untuk para pembuat keputusan.
Rekomendasi untuk Praktisi & Industri	Mendorong Tanggung Jawab Sektor Swasta. Menyerukan perbaikan dari dalam industri itu sendiri.	- Peningkatan Standar Keamanan & Kepatuhan. - Pengembangan Kode Etik Industri. - Kolaborasi Aktif dengan APH. - Inovasi Produk Syariah.	Asosiasi (ASPAKRINDO), CEO & C-Level Bursa Kripto, Pengembang Proyek Kripto, Investor Institusional.	"Pedoman Praktik Terbaik (Best Practice Guidelines)". Panduan untuk perbaikan operasional industri.

Komponen Bab 14	Fungsi Utama	Isi & Argumen Kunci	Target Audiens	Analogi Komponen
Rekomendasi untuk Akademisi & Organisasi Keagamaan	Mendorong Pengembangan Ilmu & Edukasi Masyarakat. Menyerukan peran aktif dari menara gading dan menara masjid.	- Pengembangan Kurikulum Interdisipliner. - Peningkatan Peran DSN-MUI (Ijtihad Responsif). - Literasi Digital Syariah Massif. - Mendorong Penelitian Lanjutan.	Rektor Universitas, Dekan, Dosen, Peneliti, Pimpinan Ormas Islam (MUI, NU, Muhammadiyah), Dai.	"Agenda Riset & Pengabdian Masyarakat". Arah baru untuk pengembangan ilmu dan edukasi publik.
Kata Penutup (Refleksi Akhir)	Menginspirasi & Menggugah. Memberikan makna filosofis dan visi jangka panjang di balik semua analisis teknis.	- Tanggung Jawab Bersama (*Farḍ Kifāyah*). - Visi Indonesia sebagai Pelopor Ekonomi Digital Beretika. - Ajakan untuk Terus Belajar. - Harapan & Optimisme.	Semua Pembaca. Bertujuan untuk meninggalkan kesan mendalam dan semangat positif.	"Pidato Penutup yang Menginspirasi". Mengakhiri acara dengan visi besar dan tepuk tangan.

Kontribusi Konsep Sintesis, Rekomendasi, dan Refleksi dalam Bab 14:

Konsep ini adalah puncak dari tujuan praktis dan filosofis buku ini.

1. Menghubungkan Teori dengan Praktik: Bab ini adalah jembatan terakhir yang paling eksplisit antara analisis akademis dan dunia nyata. Ia menjawab pertanyaan, "Jadi, apa gunanya semua analisis ini?" Jawabannya ada di bagian rekomendasi.
2. Memberikan "Peta Jalan" yang Jelas: Dengan membagi rekomendasi berdasarkan target audiens, bab ini memberikan panduan yang jelas dan dapat ditindaklanjuti bagi setiap pemangku kepentingan. Ini meningkatkan kemungkinan dampak nyata dari buku tersebut.
3. Memberikan Kepuasan Intelektual: Sebuah buku yang bagus tidak hanya menyajikan data dan analisis, tetapi juga menyimpulkannya dengan cara yang memuaskan dan memberikan "Aha!" momen kepada pembaca. Bagian sintesis melakukan fungsi ini.

Meninggalkan Kesan yang Abadi: Kata Penutup yang kuat memastikan bahwa pembaca tidak hanya menutup buku dan melupakannya. Sebaliknya, mereka ditinggalkan dengan sebuah visi dan perasaan menjadi bagian dari sebuah perjalanan penting, yang meningkatkan dampak jangka panjang dari karya tersebut.

Daftar Pustaka

Al-Mawardi, A. H. (1996). *Al-Ahkam as-Sultaniyyah wa al-Wilayat ad-Diniyyah*. Dar al-Kutub al-Ilmiyyah.

Al-Qaradawi, Y. (1999). *Fiqh al-Zakat: A Comparative Study*. Dar al-Taqwa.

Al-Qaradawi, Y. (2001). *The Lawful and the Prohibited in Islam*. Islamic Book Trust.

Al-Zuhaili, W. (2003). *Al-Fiqh al-Islami wa Adillatuhu*. Dar al-Fikr.

Al-Zuhaili, W. (2008). *Financial Transactions in Islamic Fiqh*. Dar al-Fikr.

ASPAKRINDO. (2022). *Pedoman Perilaku (Code of Conduct) Anggota Asosiasi Pedagang Aset Kripto Indonesia*.

Auda, J. (2008). *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach*. The International Institute of Islamic Thought.

Audah, A. Q. (2007). *Al-Tasyri' al-Jina'i al-Islami Muqaranan bi al-Qanun al-Wadh'i*. Muassasat al-Risalah.

Auer, R., & Böhme, R. (2020). The technology of retail central bank digital currency. *BIS Quarterly Review, March*.

Badan Narkotika Nasional (BNN). (2022). *Laporan Akhir Tahun 2022*. BNN.

Bank for International Settlements (BIS). (2021). *CBDCs: an opportunity for the monetary system*. Annual Economic Report.

Bank Indonesia. (2018). *Siaran Pers: BI Kembali Menegaskan Pelarangan Penggunaan Virtual Currency*. No. 20/4/DKom.

Bank Indonesia. (2022). *White Paper Proyek Garuda: Desain Konseptual Rupiah Digital*. Bank Indonesia.

Bappebti. (2020). *Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 7 Tahun 2020 tentang Penetapan Daftar Aset Kripto yang Dapat Diperdagangkan di Pasar Fisik Aset Kripto*.

Bappebti. (2021). *Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8 Tahun 2021 tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka*.

Chainalysis. (2022). *The 2022 Crypto Crime Report*. Chainalysis Inc.

Chainalysis. (2023). *The 2023 Crypto Crime Report*. Chainalysis Inc.

Chapra, M. U. (2000). *The Future of Economics: An Islamic Perspective*. The Islamic Foundation.

Chazawi, A. (2002). *Pelajaran Hukum Pidana Bagian 1*. RajaGrafindo Persada.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

Dar al-Ifta al-Misriyyah. (2018). *Fatwa on Trading in Cryptocurrency (Bitcoin)*.

Egmont Group. (2023). *List of Members*. Diakses dari https://egmontgroup.org.

European Parliament. (2023). *Markets in Crypto-Assets (MiCA) Regulation*.

Financial Action Task Force (FATF). (2020). *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*. FATF.

Financial Action Task Force (FATF). (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF.

Graaf, H. J. de. (2019). *Puncak Kekuasaan Mataram: Politik Ekspansi Sultan Agung*. (Terjemahan). Jakarta: Pustaka Alvabet.

Hadjon, P. M. (1987). *Perlindungan Hukum bagi Rakyat di Indonesia*. Bina Ilmu.

Hallaq, W. B. (2009). *An Introduction to Islamic Law*. Cambridge University Press.

Ibn Taymiyyah. (1987). *Al-Hisbah fi al-Islam*. Dar al-Kutub al-Ilmiyyah.

Interpol. (2022). *INTERPOL reports on global crime trends*. Diakses dari situs resmi Interpol.

Kamali, M. H. (2000). *Punishment in Islamic Law: An Enquiry into the Hudud Bill of Kelantan*. Ilmiah Publishers.

Kamali, M. H. (2005). *Principles of Islamic Jurisprudence*. The Islamic Texts Society.

Kamali, M. H. (2015). *The Principles of Islamic Jurisprudence*. The Islamic Texts Society.

Kejaksaan Republik Indonesia. (2020). *Laporan Tahunan Kejaksaan RI Tahun 2020*.

Kementerian Hukum dan HAM (Kemenkumham). (2019). *Laporan Kinerja Direktorat Jenderal Administrasi Hukum Umum Tahun 2019*.

Kementerian Keuangan. (2021). *Peraturan Menteri Keuangan Nomor 143/PMK.06/2021 tentang Pengelolaan Barang Milik Negara yang Berasal dari Barang Rampasan Negara dan Barang Gratifikasi*.

Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbudristek). (2021). *Buku Panduan Merdeka Belajar - Kampus Merdeka*.

Kitab Undang-Undang Hukum Pidana (KUHP).

Komite Nasional Keuangan Syariah (KNKS). (2019). *Masterplan Ekonomi Syariah Indonesia 2019-2024*.

Komite Stabilitas Sistem Keuangan (KSSK). (2020). *Laporan Stabilitas Sistem Keuangan*.

Lembaga Perlindungan Saksi dan Korban (LPSK). (2018). *Laporan Tahunan 2018*.

Majelis Ulama Indonesia (MUI). (2021). *Fatwa Nomor 74 Tahun 2021 tentang Hukum Mata Uang Kripto (Cryptocurrency)*.

Majelis Ulama Indonesia (MUI). (2021). *Himpunan Fatwa Dewan Syariah Nasional MUI*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Otoritas Jasa Keuangan (OJK). (2021). *Master Plan Sektor Jasa Keuangan Indonesia 2021-2025*.

Otoritas Jasa Keuangan (OJK). (2022). *Siaran Pers: OJK Tegaskan Larangan Penggunaan dan Fasilitasi Aset Kripto oleh Lembaga Jasa Keuangan*.

Otoritas Jasa Keuangan (OJK). (2022). *Strategi Nasional Literasi Keuangan Indonesia 2021-2025*.

Peraturan Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) No. 5 Tahun 2019 tentang Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka.

Peraturan Kapolri No. 6 Tahun 2019 tentang Penyidikan Tindak Pidana.

Polri. (2021). *Laporan Akhir Tahun 2021 Kepolisian Negara Republik Indonesia*.

Pratama, I. P. A. E. (2020). *Tantangan Penegakan Hukum Kejahatan Siber di Indonesia*. Jurnal Magister Hukum Udayana.

Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). (2022). *Laporan Tahunan 2022*. PPATK.

Saeed, A. (2016). *Islamic Banking and Finance*. Edward Elgar Publishing.

Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*, *103*(2), 153-174.

Shariah Advisory Council of the Securities Commission Malaysia. (2020). *Resolution on Digital Assets*.

Soekanto, S., & Mamudji, S. (2003). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. RajaGrafindo Persada.

Undang-Undang No. 7 Tahun 2014 tentang Perdagangan.

Undang-Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP).

Undang-Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU).

Undang-Undang No. 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme (UU PP-TPPT).

Undang-Undang No. 9 Tahun 2016 tentang Pencegahan dan Penanganan Krisis Sistem Keuangan (UU P2SK).

Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Undang-Undang No. 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.

Undang-Undang No. 35 Tahun 2009 tentang Narkotika.

Werner, S. M., Perez, D., & Gudgeon, L. (2022). *DeFi: A Comprehensive Guide*. Auerbach Publications.

World Bank. (2021). *Indonesia Economic Prospects, June 2021: The Long Road to Recovery*. The World Bank.

World Economic Forum (WEF). (2021). *DeFi Policy-Maker Toolkit*. WEF.

World Wide Web Consortium (W3C). (2022). *Decentralized Identifiers (DIDs) v1.0*. W3C Recommendation.

Zakharov, A. O. (2018). The Śrīvijayan Kingdom in the 7th–8th Centuries and Its Impact on the Political Map of Insular Southeast Asia. *Journal of the Malaysian Branch of the Royal Asiatic Society*, *90*(1), 1-24.

Glosarium

Aset Digital	:	Representasi digital dari nilai atau hak yang dapat ditransfer dan disimpan secara elektronik menggunakan teknologi *blockchain* atau DLT. Termasuk di dalamnya adalah *cryptocurrency*, token, dan NFT.
Aset Kripto	:	Istilah hukum di Indonesia untuk *cryptocurrency* yang didefinisikan oleh Bappebti sebagai komoditas yang dapat diperdagangkan di bursa berjangka.
APU-PPT	:	Singkatan dari Anti-Pencucian Uang dan Pencegahan Pendanaan Terorisme. Serangkaian kebijakan dan prosedur untuk mencegah penyalahgunaan sistem keuangan untuk kegiatan ilegal.
Baitul Mal	:	Secara harfiah berarti "rumah harta". Lembaga keuangan dalam sejarah Islam yang berfungsi sebagai kas negara untuk mengelola pendapatan dan pengeluaran demi kemaslahatan umum.
Bappebti	:	Badan Pengawas Perdagangan Berjangka Komoditi. Lembaga pemerintah di Indonesia yang bertugas mengatur dan mengawasi perdagangan fisik aset kripto.

Blockchain	:	Teknologi buku besar digital terdistribusi (*Distributed Ledger Technology* - DLT) yang mencatat transaksi dalam blok-blok yang saling terhubung dan diamankan secara kriptografis, membuatnya transparan dan sulit diubah.
Bughat	:	Pemberontakan terhadap pemimpin atau pemerintahan yang sah. Dalam fikih jinayah, ini adalah salah satu kejahatan berat.
CBDC (*Central Bank Digital Currency*)	:	Mata uang digital yang diterbitkan dan dijamin oleh bank sentral suatu negara. Contoh di Indonesia adalah Proyek Garuda untuk Rupiah Digital.
Chainalysis	:	Nama salah satu perusahaan terkemuka yang menyediakan perangkat lunak analisis *blockchain* (*blockchain analytics tools*) untuk melacak transaksi dan mengidentifikasi aktivitas ilegal.
DAO (*Decentralized Autonomous Organization*)	:	Organisasi yang dijalankan oleh aturan-aturan yang dikodekan dalam *smart contract* di *blockchain*, di mana pengambilan keputusan dilakukan oleh para pemegang token tata kelola.
Dark Web	:	Bagian dari internet yang hanya dapat diakses menggunakan perangkat lunak khusus (seperti Tor) yang memungkinkan anonimitas tinggi, sering disalahgunakan untuk pasar gelap.
DeFi (*Decentralized Finance*)	:	Ekosistem aplikasi keuangan yang dibangun di atas teknologi *blockchain* yang beroperasi tanpa perantara keuangan terpusat seperti bank.
Dittipidsiber	:	Direktorat Tindak Pidana Siber. Unit khusus di bawah Bareskrim Polri yang bertugas menangani kejahatan di dunia maya.
Dhaman	:	Prinsip ganti rugi atau pertanggungjawaban dalam hukum Islam. Pelaku kerusakan atau kerugian wajib mengganti kerugian yang diderita korban.

FATF (*Financial Action Task Force*)	:	Organisasi antarpemerintah global yang menetapkan standar internasional untuk pemberantasan pencucian uang dan pendanaan terorisme.
Fatwa	:	Pendapat atau opini hukum Islam yang dikeluarkan oleh seorang ulama atau lembaga yang memiliki otoritas (seperti MUI) sebagai jawaban atas sebuah pertanyaan.
Fintech (*Financial Technology*)	:	Inovasi teknologi yang digunakan untuk meningkatkan atau mengotomatisasi layanan dan proses keuangan.
Fiqh al-Cyber (Fikih Siber)	:	Disiplin ilmu fikih baru yang diusulkan untuk membahas secara sistematis hukum-hukum Islam yang berkaitan dengan interaksi dan aktivitas di dunia digital.
Gharar	:	Ketidakpastian, ketidakjelasan, atau ambiguitas yang berlebihan dalam sebuah transaksi, yang dilarang dalam fikih muamalah karena berpotensi merugikan salah satu pihak.
Hifzh al-Maal	:	Salah satu dari lima tujuan utama syariah (*Maqashid al-Shari'ah*), yaitu perlindungan terhadap harta.
Hirabah	:	Kejahatan perampokan atau perampasan yang disertai kekerasan dan mengganggu keamanan publik. Termasuk salah satu kejahatan *hudud* dengan sanksi yang berat.
Hudud	:	Jenis kejahatan dalam hukum pidana Islam yang jenis dan sanksinya telah ditetapkan secara spesifik dalam Al-Qur'an atau Sunnah (contoh: pencurian, perzinaan, hirabah).
I'anah 'ala al-Ma'siyah	:	Tindakan membantu atau memfasilitasi terjadinya sebuah kejahatan atau maksiat.
Ifsad fil-Ardh	:	Perbuatan membuat kerusakan di muka bumi. Kategori kejahatan luas yang mencakup tindakan-tindakan yang merusak tatanan sosial, keamanan, dan lingkungan.

Ijtihad	:	Upaya sungguh-sungguh yang dilakukan oleh seorang ahli hukum Islam (*mujtahid*) untuk menyimpulkan hukum syariah dari sumber-sumbernya untuk kasus-kasus baru.
Ishlah	:	Prinsip perbaikan atau rekonsiliasi. Dalam konteks hukum, sering merujuk pada pendekatan keadilan restoratif.
Itqan	:	Prinsip profesionalisme, kesempurnaan, dan melakukan sesuatu dengan cara terbaik.
Jarimah	:	Istilah umum dalam bahasa Arab untuk tindak pidana atau kejahatan.
Koin (*Coin*)	:	Aset kripto asli dari sebuah jaringan *blockchain* (contoh: Bitcoin di jaringan Bitcoin, Ether di jaringan Ethereum) yang berfungsi sebagai alat pembayaran atau gas fee di dalam jaringan tersebut.
Kriptografi	:	Ilmu tentang teknik penyandian untuk mengamankan komunikasi dan data. Menjadi dasar keamanan dalam teknologi *blockchain*.
KYC (*Know Your Customer*)	:	Prinsip Mengenali Pengguna Jasa. Proses yang wajib dilakukan oleh lembaga keuangan untuk memverifikasi identitas nasabahnya guna mencegah pencucian uang.
Maqashid al-Shari'ah	:	Tujuan-tujuan fundamental di balik ditetapkannya hukum Islam, yang paling utama adalah perlindungan terhadap agama, jiwa, akal, keturunan, dan harta.
Maslahah 'Ammah	:	Kemaslahatan atau kepentingan umum. Salah satu pertimbangan utama dalam penetapan hukum Islam, terutama dalam ranah *ta'zir* dan kebijakan publik.
Maysir	:	Perjudian atau spekulasi untung-untungan, yang dilarang dalam Islam.
MLA (*Mutual Legal Assistance*)	:	Perjanjian Bantuan Hukum Timbal Balik. Mekanisme kerja sama formal antarnegara untuk meminta dan memberikan bantuan dalam penegakan hukum.
Mufsid fil-Ardh	:	Orang yang melakukan kerusakan di muka bumi.

Mutaqawwim	:	Harta yang memiliki nilai dan diakui oleh syariah, sehingga sah untuk dimiliki dan ditransaksikan.
Nash	:	Teks suci yang menjadi sumber hukum primer dalam Islam, yaitu Al-Qur'an dan Sunnah.
NFT (Non-Fungible Token)	:	Token kriptografis unik di *blockchain* yang merepresentasikan kepemilikan atas aset tertentu, baik digital maupun fisik, dan tidak dapat dipertukarkan satu sama lain.
PFAK (Pedagang Fisik Aset Kripto)	:	Istilah Bappebti untuk perusahaan yang telah mendapatkan izin untuk menyelenggarakan jual beli aset kripto di Indonesia, atau yang biasa dikenal sebagai bursa kripto (*exchange*).
Phishing	:	Tindakan penipuan untuk mencuri informasi sensitif seperti kata sandi atau *private key* dengan menyamar sebagai entitas tepercaya.
PPATK	:	Pusat Pelaporan dan Analisis Transaksi Keuangan. Unit intelijen keuangan (*Financial Intelligence Unit* - FIU) Indonesia.
Private Key	:	Kunci pribadi. Sebaris data kriptografis rahasia yang memungkinkan pemiliknya untuk mengakses dan mengontrol aset kripto di sebuah alamat *blockchain*. Kehilangan *private key* berarti kehilangan akses ke aset tersebut.
Qarinah	:	Petunjuk atau bukti tidak langsung (*ind circumstantial evidence*) yang dapat digunakan untuk memperkuat pembuktian dalam hukum acara Islam.
Qiyas	:	Analogi. Salah satu metode penetapan hukum Islam untuk kasus baru dengan cara menganalogikannya pada kasus lama yang sudah ada hukumnya di dalam *nash*, berdasarkan kesamaan 'illah (alasan hukum).
Qisas	:	Hukuman balasan yang setimpal, terutama untuk kejahatan terhadap jiwa dan badan (pembunuhan dan penganiayaan).

RegTech (*Regulatory Technology*)	:	Penggunaan teknologi oleh perusahaan untuk mematuhi peraturan secara lebih efisien.
Restitusi	:	Pengembalian harta atau pembayaran ganti rugi kepada korban kejahatan.
Riba	:	Bunga atau tambahan yang disyaratkan dalam transaksi pinjam-meminjam atau jual beli barang ribawi. Diharamkan dalam Islam.
Rug Pull	:	Jenis penipuan di dunia kripto di mana pengembang sebuah proyek tiba-tiba meninggalkan proyek tersebut dan membawa kabur seluruh dana investor.
Sadd al-Dzari'ah	:	Prinsip pencegahan dalam hukum Islam, yaitu menutup jalan atau sarana yang dapat menuju kepada perbuatan yang dilarang.
Sariqah	:	Pencurian. Dalam fikih, dibedakan antara *sariqah hudud* (yang memenuhi syarat untuk sanksi potong tangan) dan *sariqah ta'ziriyah* (yang sanksinya ditentukan hakim).
Shitcoin	:	Istilah slang (peyoratif) untuk aset kripto yang tidak memiliki nilai, tujuan, atau utilitas yang jelas, sering kali dibuat untuk tujuan penipuan.
Siyasah Syar'iyyah	:	Kebijakan publik yang dibuat oleh pemerintah yang sejalan dengan prinsip-prinsip syariah untuk mewujudkan kemaslahatan umum.
Smart Contract	:	Program komputer atau protokol transaksi yang secara otomatis mengeksekusi, mengontrol, atau mendokumentasikan tindakan dan peristiwa yang relevan secara hukum sesuai dengan ketentuan perjanjian.
SupTech (*Supervisory Technology*)	:	Penggunaan teknologi oleh lembaga regulator untuk meningkatkan efektivitas dan efisiensi pengawasan.

Ta'zir	:	Jenis kejahatan dalam hukum pidana Islam yang jenis dan sanksinya tidak ditetapkan dalam *nash*, melainkan diserahkan kepada kebijakan penguasa (*ulil amri*) atau hakim.
Tadlis	:	Tindakan menyembunyikan cacat atau memberikan informasi palsu dalam sebuah transaksi untuk menipu pihak lain.
Tasyhir	:	Sanksi berupa publikasi atau pengumuman kejahatan seseorang kepada publik untuk memberikan efek jera dan peringatan bagi yang lain.
Token	:	Aset kripto yang dibangun di atas jaringan *blockchain* yang sudah ada (misalnya, token ERC-20 di jaringan Ethereum). Dapat merepresentasikan berbagai hal, seperti utilitas, sekuritas, atau aset riil.
TPPU	:	Tindak Pidana Pencucian Uang.
Ulil Amr	:	Pemegang kekuasaan atau otoritas dalam suatu negara atau komunitas, yaitu pemerintah yang sah.

Indeks

A

B

C

D

E

F

G

H

I

J

K

L

M

N

P

Q

R

S

T

U

W

Biodata Penulis

Dr. R. Arif Muljohadi, S.H., M.Hum., adalah Praktisi dan akademisi di bidang Ilmu Hukum. Lulus Sarjana Hukum dari Universitas Bangkalan, Madura (Universitas Trunojoyo Madura), dan Magister Ilmu Hukum dari Universitas Wijaya Kusuma, Surabaya (2005), serta Doktor Ilmu Hukum dari Universitas 17 Agustus 1945, Surabaya (2022). Penulis mengajar di Program Studi Hukum Pidana Islam dan saat ini tercatat sebagai dosen tetap di Institut Agama Islam Syaichona Mohammad Cholil Bangkalan, Madura. Selain aktif mengajar, melakukan penelitian dan pemateri di berbagai seminar, penulis juga sebagai Advokat dan Konsultan Hukum beberapa Perusahaan di Indonesia. Penulis juga menjabat sebagai Ketua Bidang Advokasi dan HAM Forum Silaturrahmi Doktor Indonesia (FORSILADI) Jawa Timur, Pengurus Ikatan Cendekiawan Muslim (ICMI) Orwil Jawa Timur dan menjabat sebagai Pengurus Bidang LITBANG Perhimpunan Advokat Indonesia (PERADI) Surabaya. Penulis merupakan anggota ASPERHUPIKI (Asosiasi Pengajar Hukum Pidana dan Kriminologi).

Mulyohadi, R.Arif
Institut Agama Islam Syaichona Mohammad Cholil Bangkalan
Madura, Indonesia
Scopus ID: 59667792400

Catatan

MENGUNGKAP RAHASIA CRYPTOCURRENCY

Perspektif Hukum Pidana Islam

dalam Menanggulangi Kejahatan Ekonomi Digital

Di tengah euforia dan disrupsi ekonomi digital, *cryptocurrency* muncul sebagai pedang bermata dua. Di satu sisi, ia menjanjikan revolusi keuangan melalui teknologi blockchain yang transparan dan terdesentralisasi. Di sisi lain, sifatnya yang anonim dan tanpa batas telah membuka kotak pandora bagi modus-modus kejahatan ekonomi modern yang semakin canggih, mulai dari penipuan investasi berskala masif, pencucian uang lintas negara, hingga pendanaan terorisme yang sulit dilacak. Fenomena ini tidak hanya menjadi tantangan bagi hukum positif Indonesia, tetapi juga mengajukan pertanyaan fundamental bagi hukum pidana Islam (*fiqh al-jinâyah*): Mampukah kerangka hukum yang berakar pada tradisi menjawab kejahatan yang lahir dari rahim teknologi abad ke-21?

Buku referensi definitif ini menjawab tantangan tersebut dengan melakukan analisis multidisipliner yang mendalam, memadukan ketajaman ilmu hukum, teknologi, ekonomi, dan fikih Islam. Perjalanan dimulai dengan membedah anatomi cryptocurrency dan evolusi ekonomi digital, memetakan potensi inovasi sekaligus risiko yang menyertainya. Buku ini kemudian mengupas tuntas berbagai modus operandi kejahatan—mulai dari skema Ponzi berkedok robot trading, pencucian uang oleh *influencer*, peretasan bursa kripto, hingga transaksi narkotika di *dark web*—melalui studi kasus nyata yang terjadi di Indonesia.

Inti dari buku ini adalah analisis dua pilar hukum: hukum positif Indonesia dan hukum pidana Islam. Pembaca akan diajak menelusuri bagaimana perangkat hukum nasional, seperti KUHP, UU ITE, dan UU TPPU, berupaya menjerat para pelaku, sekaligus mengidentifikasi keterbatasan dan celah yang ada. Secara paralel, buku ini melakukan ijtihad intelektual dengan menunjukkan bagaimana prinsip-prinsip hukum pidana Islam, khususnya melalui konsep *jarîmah ta'zîr* (delik yang sanksinya ditentukan oleh penguasa), memiliki fleksibilitas yang luar biasa untuk mengkualifikasikan setiap kejahatan digital modern sebagai tindak pidana yang layak dihukum.

Lebih dari sekadar analisis, karya ini menawarkan sebuah sintesis. Buku ini secara cermat mempertemukan titik-titik temu filosofis dan praktis antara *Maqashid al-Syari'ah* (tujuan-tujuan luhur hukum Islam) dan tujuan hukum nasional, membuktikan bahwa keduanya dapat berjalan harmonis. Puncaknya, buku ini merumuskan strategi penanggulangan yang holistik, mencakup langkah-langkah preventif (edukasi dan penguatan regulasi), represif (peningkatan kapasitas aparat penegak hukum), hingga rekomendasi kebijakan konkret bagi pemerintah, industri, akademisi, dan organisasi keagamaan.

Ditulis dengan bahasa akademis yang presisi namun tetap mudah dipahami, buku ini tidak hanya ditujukan bagi para ahli hukum dan praktisi, tetapi juga bagi mahasiswa, regulator, investor, dan siapa saja yang ingin memahami persimpangan krusial antara teknologi, kejahatan, dan keadilan di era digital. Ini adalah sebuah panduan esensial untuk menavigasi masa depan keuangan, sebuah ajakan untuk membangun ekosistem ekonomi digital Indonesia yang tidak hanya inovatif, tetapi juga aman, adil, dan membawa kemaslahatan bagi semua.

SAMUDRA SOLUSI PROFESIONAL
CV. SAMUDRA SOLUSI PROFESIONAL

Alamat Kantor:
Pusat:
[illegible]
Cabang:
[illegible]

ISBN 978-634-7296-94-8