

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Pengaturan Teknologi *Blockchain* Dalam Upaya Penanggulangan Kecurangan Pembayaran Melalui QRIS Yang Dilakukan Oleh Konsumen Dalam Transaksi Elektronik

1. Pengaturan Teknologi *Blockchain* Menurut Peraturan Otoritas Jasa Keuangan (OJK)

Peraturan Otoritas Jasa Keuangan (OJK) Nomor 13/PJOK.02/2007 mengenai Layanan Keuangan Berbasis Teknologi Informasi merujuk pada pengaturan terkait penerapan teknologi *blockchain* dalam layanan keuangan, yang sering dikenal sebagai financial technology (fintech). Hal ini mencerminkan upaya OJK dalam mengakomodasi perkembangan teknologi di sektor keuangan. Dengan demikian, peraturan tersebut memberikan kerangka kerja yang jelas bagi pelaku industri fintech dalam menggunakan teknologi *blockchain* untuk menyediakan layanan keuangan. Ini merupakan langkah signifikan dalam memperkuat infrastruktur teknologi keuangan di Indonesia dan memfasilitasi inovasi dalam sektor tersebut.

Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 37/POJK.04/2018, yang mengatur layanan urus dana melalui penawaran saham berbasis teknologi informasi (*Equity Crowdfunding*), yang lebih dikenal sebagai Peraturan OJK 37/POJK.04/2018, merupakan panduan kebijakan regulasi selanjutnya terkait penggunaan *blockchain* dalam

penawaran saham yang didasarkan pada teknologi. Regulasi ini mengakui *blockchain* sebagai teknologi pendukung yang dapat meningkatkan kualitas layanan urun dana. Meskipun fokus pada penawaran saham berbasis teknologi, aturan ini membuka peluang untuk mendefinisikan *blockchain* secara hukum, di mana pada Pasal 47, "*Blockchain*" didefinisikan sebagai layanan pembukuan yang berkaitan dengan transaksi keuangan yang menggunakan Teknologi Informasi untuk mencatat dan menyimpan data bukti transaksi atau ledger secara terdistribusi menggunakan jaringan komputer, baik dalam skala privat maupun publik. Gabungan dua kebijakan regulasi ini dianggap memiliki kekuatan hukum yang setara dengan peraturan perundang-undangan di Indonesia. Namun, penjelasan dalam lampiran Peraturan OJK 37/POJK.04/2018 perlu dianalisis lebih lanjut, karena tidak memiliki kekuatan hukum mengikat seperti bagian inti dari peraturan perundang-undangan, dan hanya digunakan untuk memperjelas norma. Oleh karena itu, kedua regulasi tersebut tidak memadai sebagai dasar hukum yang cukup untuk mengembangkan penerapan *blockchain* di Indonesia. Perlunya regulasi yang lebih baik menjadi prioritas, yang sejalan dalam konteks politik hukum siber di Indonesia untuk memperoleh manfaat dari teknologi sekaligus mencegah penyalahgunaannya dengan mempertahankan nilai-nilai masyarakat seperti kepastian hukum, keuntungan, kehati-hatian, itikad baik, dan kebebasan untuk tetap netral terhadap teknologi.⁶¹

⁶¹ Satria Muhammad Nur Lase, Aisyah Adinda, Rizkia Diffa Yuliantika, "Kerangka Hukum Teknologi Blockchain berdasarkan Hukum Siber di Indonesia" *Padjadjaran Law Review*, Vol 9, no. 1 (2021): 9-10

Pelaksanaan dari ketentuan-ketentuan tersebut melibatkan penerapan praktik-praktik yang diatur dalam peraturan, di mana teknologi *blockchain* hadir sebagai salah satu alat penting dalam penegakan hukum yang efektif. Peningkatan pemahaman dan kesadaran hukum masyarakat terkait peningkatan layanan perbankan yang menggunakan pembayaran non-tunai melalui QRIS dapat diperkuat melalui sosialisasi yang luas dan pelatihan yang intensif. Hal ini penting karena transaksi digital sekarang merupakan bagian penting dari kehidupan sehari-hari dan memiliki berdampak besar dalam perekonomian. Dengan memahami tata cara penggunaan QRIS dan risiko yang terkait, masyarakat akan lebih waspada dalam bertransaksi, sementara pengetahuan tentang potensi tindak pidana akan memperkuat upaya pencegahan kejahatan. Perlindungan hukum yang holistik, meliputi aspek preventif dan represif, juga penting untuk memberikan jaminan keamanan dan kepercayaan dalam transaksi digital, dengan melibatkan partisipasi aktif masyarakat serta meningkatkan kapasitas dan infrastruktur untuk aparat penegak hukum.⁶² Terakhir, upaya penanggulangan dilakukan melalui langkah-langkah konkret, seperti pemanfaatan teknologi *blockchain* untuk memastikan integritas transaksi dan mencegah manipulasi data yang merugikan konsumen. Dengan demikian, pengaturan ini mencakup aspek-aspek penting dalam menjaga keamanan dan kepercayaan dalam transaksi

⁶² Mas Rara Tri Retno Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia." *Rechtsidee* Vol 11, no. 1 (2023): 10

elektronik, khususnya melalui QRIS, serta menunjukkan komitmen untuk melindungi konsumen dari tindakan kecurangan yang merugikan.

2. Pengaturan Perbuatan Curang Menurut Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang ITE

a. Pengaturan Perbuatan Curang dalam Kitab Undang-Undang Hukum Pidana (KUHP)

Kitab Undang-Undang Hukum Pidana (KUHP) mencakup berbagai tindakan yang dikategorikan sebagai perbuatan curang (*fraud*). Beberapa pasal yang relevan antara lain:⁶³

- 1) Pasal 362: Mengatur tentang mengambil barang milik orang lain, baik sebagian maupun keseluruhan, dengan tujuan untuk memiliki secara tidak sah.
- 2) Pasal 368: Mengatur tentang pemerasan dan pengancaman didefinisikan sebagai tindakan memaksa seseorang dengan menggunakan kekerasan atau memberikan ancaman kekerasan untuk memberikan barang yang sebagian atau seluruhnya milik orang tersebut atau orang lain, atau untuk membuat utang atau menghapuskan piutang, dengan tujuan menguntungkan diri sendiri atau orang lain secara tidak sah.
- 3) Pasal 372: Mengatur tentang penggelapan didefinisikan sebagai memiliki barang yang milik orang lain sebagian atau seluruhnya,

⁶³ Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP)

secara sengaja dan melanggar hukum, namun barang tersebut berada dalam kekuasaannya bukan karena tindakan kejahatan.

- 4) Pasal 378: Mengatur tentang perbuatan curang didefinisikan sebagai tindakan memanfaatkan nama palsu atau martabat palsu, menggunakan tipu daya atau rangkaian kebohongan, dengan tujuan menguntungkan diri sendiri atau orang lain secara tidak sah, untuk menggerakkan orang lain agar menyerahkan barang kepada pelaku, atau agar memberikan utang atau menghapuskan piutang.
- 5) Pasal 396: Mengatur tindakan yang merugikan pemberi piutang dalam keadaan bangkrut .
- 6) Pasal 406: Mengatur tentang penghancuran atau perusakan barang.

Kemunculan teknologi *blockchain* telah membawa perubahan paradigma di berbagai sektor, termasuk dalam konteks hukum pidana di Indonesia. Karakteristik desentralisasi, ketidakbisaan untuk diubah, dan transparansi yang dimiliki oleh *blockchain* memberikan peluang serta tantangan baru dalam implementasi Kitab Undang-Undang Hukum Pidana (KUHP) di negara ini. Meskipun KUHP tidak secara tegas mengatur tentang teknologi *blockchain*, beberapa pasal didalamnya dapat diartikan untuk mencakup aktivitas yang terkait dengan teknologi ini. Sebagai contoh, Pasal 378 KUHP tentang Penipuan dapat diterapkan dalam kasus penipuan yang terkait dengan *cryptocurrency*, aset digital, dan investasi menggunakan teknologi *blockchain*. Demikian pula, Pasal 280 KUHP mengenai Pencemaran Nama Baik relevan untuk menangani

penyebaran informasi palsu atau menyesatkan melalui platform *blockchain*. Selain itu, Pasal-pasal lain seperti Pasal 321 KUHP tentang Perbuatan Merusak, Pasal 372 KUHP tentang Penggelapan, dan Pasal 82 KUHP tentang Pidana Membantu Melakukan Kejahatan juga memiliki relevansi dalam konteks penegakan hukum terkait dengan *blockchain*. Pasal-pasal tersebut dapat digunakan untuk menangani tindakan yang merusak jaringan *blockchain*, penggelapan aset digital dalam bentuk *cryptocurrency* dan NFT, serta penyalahgunaan kekuasaan untuk keuntungan pribadi terkait dengan teknologi *blockchain*.⁶⁴

Dengan demikian, walaupun belum ada regulasi yang secara khusus mengatur *blockchain*, KUHP memberikan landasan hukum yang dapat digunakan untuk menegakkan hukum dalam kasus-kasus yang melibatkan teknologi ini. Namun, penting untuk terus mengkaji dan mengembangkan kerangka hukum yang lebih spesifik untuk menanggapi perkembangan teknologi *blockchain* secara efektif dan adil.

Dalam konteks transaksi *blockchain*, perlu dipertimbangkan perspektif hukum kebendaan yang mengatur hak milik dan pengakuan atas benda, termasuk benda tidak berwujud. Meskipun pasal 499 KUH Perdata mendefinisikan benda sebagai barang dan hak yang dapat menjadi objek hak milik, hukum benda tersebut tidak secara khusus

⁶⁴ Ahmad Sofian, Bambang Pratama, "Tindak Pidana Mata Uang dalam Konteks Hukum Pidana dan Hukum Siber" *Jurnal Hukum Pidana dan Kriminologi*, 2, no. 2 (2021): 57

mengakui benda tidak berwujud. Namun, pengakuan atas benda tak berwujud yang bergerak diatur dalam Pasal 16 (1) Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, yang menyatakan bahwa hak cipta merupakan benda bergerak tidak berwujud. Dalam hal ini, transaksi blockchain dilihat sebagai perbuatan hukum yang diatur oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik mendefinisikan transaksi elektronik sebagai tindakan hukum yang dilakukan melalui penggunaan komputer, jaringan komputer, dan/atau media elektronik lainnya. Oleh karena itu, walaupun hukum kebendaan tidak secara langsung mengakui transaksi blockchain, undang-undang yang terkait dengan transaksi elektronik memberikan kerangka hukum yang relevan bagi pengaturan dan pengakuan transaksi blockchain dalam konteks hukum kebendaan.⁶⁵

b. Pengaturan Perbuatan Curang dalam Undang-Undang ITE

Undang-Undang ITE juga mengatur tindakan kecurangan yang dilakukan melalui media elektronik. Beberapa pasal yang relevan dalam UU ITE meliputi:

- 1) Pasal 28 ayat (1) menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak menyebarkan informasi palsu dan menyesatkan yang menyebabkan kerugian bagi konsumen dalam transaksi elektronik."

⁶⁵ Edwin Rachmad Fajarianto, Pandri Zulfikar, Edi Mulyadi, "Tinjauan Yuridis Penggunaan Blockchain-Smart Contract Dalam Transaksi Non-Fungible Token (Nft) Pada Pt. Saga Riung Investama." *Jurnal Pemandhu* ,3, no. 2 (2022): 89

- 2) Pasal 35: Pasal ini mengatur tentang manipulasi informasi elektronik, yang menyatakan bahwa "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik."
- 3) Pasal 36: Pasal ini menambahkan bahwa pelaku yang menyebabkan kerugian bagi orang lain dengan cara-cara tersebut dapat dikenai hukuman tambahan.⁶⁶

Legislatif di Indonesia sudah mulai mengakui pentingnya teknologi *blockchain* dalam ranah hukum. Sebagai contoh, perubahan yang dibawa oleh Undang-Undang Nomor 10 Tahun 2020 terhadap Undang-Undang Nomor 1 Tahun 2009 tentang Informasi dan Transaksi Elektronik (UU ITE), memberikan dasar hukum untuk penggunaan teknologi *blockchain* dalam transaksi elektronik. Dengan demikian, teknologi *blockchain* dapat menjadi landasan hukum yang kuat untuk transaksi kontrak di Indonesia.⁶⁷

UU ITE belum secara langsung mengatur teknologi *blockchain*, tetapi beberapa ketentuannya dianggap menjadi dasar hukum untuk

⁶⁶ Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

⁶⁷ Leny Megawati, Cecep Wiharma, Asep Hasanudin, "Peran Teknologi Blockchain Dalam Meningkatkan Keamanan Dan Kepastian Hukum Dalam Transaksi Kontrak Di Indonesia." *Jurnal Hukum Mimbar Justitia* , 9 , no. 2 (2023): 412

aktivitas yang melibatkan *blockchain* di Indonesia. UU ITE (UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik) menjadi dasar legalitas yang mengatur aktivitas di ruang digital, termasuk yang mungkin melibatkan *blockchain*. Meskipun belum ada regulasi yang spesifik, peraturan lain terkait penyelenggaraan transaksi elektronik seperti Peraturan Pemerintah (PP) terkait Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) (PP No. 71 Tahun 2019) dan Perdagangan Melalui Sistem Elektronik (PMSE) (PP No. 80 Tahun 2019) juga memiliki dampak yang signifikan. Beberapa pasal dalam UU ITE dapat diinterpretasikan untuk menangani tindak pidana terkait aktivitas *blockchain*, seperti Pasal 28 tentang Larangan Melakukan Transaksi yang Melanggar Hukum dan Pasal 29 tentang Penyebaran Informasi yang Menyesatkan. Namun, para ahli hukum menyoroti pentingnya regulasi yang lebih spesifik untuk *blockchain* guna menciptakan kepastian hukum dan melindungi konsumen. Sebagai contoh, Peraturan Menteri Komunikasi dan Informatika Nomor 3 Tahun 2021 tentang Standar Kegiatan Usaha dan Standar Produk dalam Perizinan Berusaha Berbasis Risiko di Sektor Pos, Telekomunikasi, dan Sistem dan Transaksi Elektronik juga mencakup standarisasi terkait penyelenggaraan sistem berbasis *blockchain*.⁶⁸

⁶⁸ Muhammad Habiburrahman, Muhaimin, Abdul Atsar, "Perlindungan Hukum Bagi Pengguna Transaksi Cryptocurrency Di Indonesia." *Jurnal Education And Development*, 10, no. 2 (2022): 701-702

3. Pelaksanaan Studi Kasus Terkait Perbuatan Curang Yang Dilakukan Konsumen Terhadap Pelaku Usaha

Melakukan pembayaran melalui QRIS tidak selalu memberikan dampak positifnya bagi kedua belah pihak, namun setiap pihak juga memiliki potensi risiko kerugian sebagai konsekuensinya. Adanya kerugian yang ditimbulkan bukan hanya bisa berasal dari secara *face to face*, namun dari QR scan pada QRIS juga dapat menimbulkan penipuan seperti barcode palsu atau pada saat melakukan scan barcode yang mana autentifikasinya berhasil namun tidak menghasilkan uang sama sekali dari scan yang sudah dilakukan. Dalam penelitian penulis mengambil tiga sumber wawancara yaitu pemilik warung makan, pemilik franchise UMKM, dan pegawai toko kelontong. Dari ketiga pelaku usaha tersebut mereka menyediakan layanan QRIS karena mengikuti dengan adanya perkembangan zaman dan lokasi usaha mereka bertepatan di pusat kota, sehingga dengan hal tersebut dapat memudahkan pengunjung ataupun pembeli dalam melakukan pembayaran.⁶⁹

1. Nama Pelaku usaha : Ibu Tiara Dewandari (pemilik warung makan “Numani”)

Kronologi kasus:

Pada saat jam makan siang langganan konsumen warung makan “Numani” berbondong-bondong makan siang di warung

⁶⁹ Rahmanto, Tony Yuri, J. H. R. S. Kav, dan J. S. Kuningan. "Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik." *Jurnal Penelitian Hukum De Jure* 19, No. 1 (2019)

tersebut. Dikarenakan kondisi warung tersebut rame pada saat itu ada pembeli yang menggunakan kesempatan tersebut ingin membayar melalui QRIS dengan menunjukkan bukti pembayaran palsu melalui QRIS sejumlah Rp 36.000.00 sesuai dengan total yang dibeli pembeli tersebut, pada saat itu memang warung sedang ramai jadi si pemilik tidak melihat dengan detail. Pada malam hari si pemilik melihat pemasukan transaksi dari QRIS tersebut bahwa belum ada masuk senilai Rp 36.000.00 tersebut. Pemilik warung mengira bahwa sistemnya sedang eror maka kemungkinan lama masuk, namun beberapa hari tidak ada yang masuk. Setelah itu si pemilik mengetahui pacar dari si pembeli tersebut dan bicara dengan pacarnya, dengan merasa bersalah pacarnya membayar sebesar Rp 36.000.00 tersebut.⁷⁰

Dengan sistem eror tersebut mungkin bisa terjadi pada aplikasi yang tidak memiliki integritas yang kuat seperti bank yang telah dipantau oleh Otoritas Jasa Keuangan (OJK), contohnya seperti aplikasi Dana.⁷¹ Pembayaran menggunakan scan QRIS melalui dana dapat membahayakan dan memberikan kerugian bersifat nominal pada penjual karena aplikasi dana tidak diawasi oleh OJK atau izin guna aplikasi Dana tidak terintergritas oleh OJK lagi, sehingga penipuan dari aplikasi Dana sangatlah mudah dilaksanakan, karena tidak ada pengawas

⁷⁰ Hasil wawancara pelaku usaha pertama pukul 13.00 WIB

⁷¹ Hartanto, Vincent Rosadi, Ervin Alvaro Yosmar "Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana" *PATTIMURA Legal Journal*, Vol 2, no 3 (2023): 273

Badan Keuangan. Pengaturan yang ada di dalam OJK dalam pengawasan aplikasi tersebut sangat minim, karena hanya diawasi oleh Kominfo dan Bank Indonesia. Selain itu juga kurangnya sistem *Blockchain* menjadi salah satu faktor yang menyebabkan situasi tersebut negara-negara maju berbondong-bondong memajukan sistem *Blockchain* dikarenakan dengan *Blockchain* semakin memperkuat penggunaan layanan digital pada sistem keuangan sehingga meminimalisir penipuan via dompet online.

Dalam kasus Ibu Tiara Dewandari sebagai pemilik warung makan "Numani", OJK bertanggung jawab untuk memberikan pedoman dan regulasi yang jelas kepada pelaku usaha mengenai tata cara penggunaan QRIS dan langkah-langkah pencegahan kecurangan. OJK juga memiliki peran dalam memberikan pelatihan dan sosialisasi kepada pelaku usaha untuk meningkatkan pemahaman mereka tentang teknologi *blockchain* sebagai solusi dalam memperkuat keamanan transaksi elektronik, serta bagaimana cara menggunakan QRIS dengan bijaksana. Dengan demikian, OJK dapat membantu pelaku usaha seperti Ibu Tiara Dewandari untuk mengatasi atau mencegah masalah seperti yang terjadi dalam kronologi kasus tersebut, serta meningkatkan kepercayaan masyarakat terhadap transaksi elektronik yang dilakukan melalui QRIS.

Selain pelaku usaha pertama ada juga modus penipuan QRIS palsu yang dialami oleh pelaku usaha kedua yakni :

2. Nama pelaku usaha : Andre (karyawan toko kelontong)

Kronologi kasus:

Pada saat malam hari ada pembeli yang datang ke tokonya dengan berniat untuk melakukan kecurangan, disaat konsumen tersebut melihat penjaganya sedang mengantuk disitulah konsumen berkesempatan dengan melakukan pemalsuan pembayaran melalui QRIS sebesar Rp 50.000.00. Pada saat itu Andre yang menjaga kasir dan sedang shift malam diantara jam 02.00 – 03.00 dini hari Andre tidak mengecek transaksi masuk lagi dikarenakan setengah sadar mengantuk. Pada saat pagi hari setelah di cross check oleh Andre dengan catatan buku yang ditulisnya, ada pembayaran yang tidak masuk dalam transaksi pembayaran melalui QRIS sebesar Rp 50.000.00 tersebut dan akhirnya Andre ingin mengecek kembali pada keesokan hari untuk memastikan kembali, namun memang belum ada masuk sebesar Rp 50.000.00 di tanggal dan jam saat pembeli tersebut membeli dan membayar, dikarenakan Andre mengakui teledor tidak mengecek kembali pada riwayat pemasukan melalui QRIS maka mau tidak mau Andre harus membayar kerugian Rp 50.000.00 tersebut dengan uang pribadinya.⁷²

Dalam hal ini walau nominal kecil, hal ini sudah termasuk dalam penipuan berbasis transaksi elektronik. Semua pihak, termasuk

⁷² Hasil wawancara pelaku usaha kedua pada pukul 16.10 WIB

pemerintah, lembaga penegak hukum, dan komunitas, memiliki peran yang adil dalam upaya pencegahan kriminal.⁷³ Menurut G. Peter Hoefnagels, penanggulangan kejahatan dapat dilakukan melalui penerapan hukum pidana, tindakan pencegahan tanpa pidana, dan pengaruh terhadap persepsi masyarakat tentang kejahatan dan hukuman melalui media massa.

Selain yang dialami oleh pelaku usaha pertama dan kedua terkait modus penipuan pembayaran melalui QRIS, pelaku usaha ketiga juga mengalami hal berikut:

3. Nama pelaku usaha : Dwi (pemilik usaha mitra UMKM)

Kronologi kasus:

Setiap hari, pelaku usaha menjual produk-produk seperti telur gulung dan cilor tusuk. Usaha ini merupakan bagian dari mitra UMKM sebuah minimarket. Pada hari kejadian, Dwi, pelaku usaha tersebut, berjualan di depan minimarket dan melayani pembeli seperti biasanya. Sebagian besar pembeli, terutama dari kalangan muda, menggunakan QRIS untuk melakukan pembayaran. Namun, Dwi mengalami kerugian akibat tindakan penipuan oleh salah satu konsumen yang memang berniat untuk menipu. Konsumen tersebut melakukan pembayaran dengan memindai barcode QRIS yang disediakan dan menunjukkan bukti pembayaran kepada Dwi.

⁷³ Rahmad, Noor. "Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online." Jurnal Hukum Ekonomi Syariah 3, No. 2 (2019)

Namun, Dwi tidak memeriksa notifikasi pembayaran yang masuk di telepon genggamnya secara rinci. Akibatnya, Dwi mengalami kerugian sebesar Rp 40.000,00. Dwi menyatakan, “Memang kesalahan saya jarang sekali untuk mengecek kembali notifikasi yang masuk jika ada pembeli yang melakukan pembayaran melalui QRIS.” Kejadian ini menunjukkan bahwa konsumen tersebut secara sengaja memanfaatkan situasi untuk melakukan penipuan.⁷⁴

Dengan kejadian yang dialami tersebut, Dwi lebih berhati-hati lagi jika ada pembeli yang melakukan pembayaran melalui QRIS dan menunjukkan bukti pembayaran, Dwi selalu mengecek notifikasi pembayaran yang masuk untuk menghindari kerugian yang telah dialami.⁷⁵

Kasus penipuan melalui QRIS yang dialami Dwi, pemilik usaha mitra UMKM, menjadi contoh nyata modus operandi yang sering terjadi. Dwi yang berjualan di depan minimarket, tertipu oleh pembeli yang menggunakan metode pembayaran melalui QRIS dengan menunjukkan bukti pembayaran palsu. Ketidaktelitian Dwi dalam mengecek notifikasi pembayaran di handphone-nya menjadi celah untuk pelaku penipuan. Akibatnya, Dwi mengalami kerugian sebesar Rp 40.000.

⁷⁴ Hasil wawancara pada pelaku usaha ketiga pukul 19.00 WIB

⁷⁵ Hasil wawancara pada pelaku usaha ketiga pukul 19.00 WIB

Modus penipuan melalui QRIS ini tergolong sederhana namun efektif bagi pembeli yang memanfaatkan kelengahan korban dengan menunjukkan bukti pembayaran palsu. Dalam kasus Dwi, pembeli kemungkinan menggunakan aplikasi edit gambar atau screenshot bukti pembayaran dari transaksi lain. Modus tersebut merupakan tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP.

Kasus Dwi menjadi pengingat bagi para pelaku usaha, khususnya UMKM untuk selalu waspada dan berhati-hati dalam menerima pembayaran melalui QRIS. Ketidaktelitian dan kurangnya edukasi tentang modus penipuan online dapat mengakibatkan kerugian finansial. Untuk mencegah penipuan melalui QRIS, beberapa langkah dapat dilakukan, seperti memastikan keaslian bukti pembayaran dan selalu mengecek notifikasi pembayaran.

Kasus Dwi menunjukkan pentingnya edukasi dan kewaspadaan dalam bertantraksi online. Pelaku usaha perlu meningkatkan pengetahuannya tentang modus penipuan online dan menerapkan langkah-langkah pencegahan untuk melindungi diri dari kerugian. Selain itu, pelaporan kasus penipuan ke pihak berwajib dapat membantu proses investigasi dan penjeratan pelaku. Kesimpulannya, penipuan melalui QRIS dapat dicegah dengan edukasi, kewaspadaan, dan langkah-langkah pencegahan yang tepat.

4. Upaya Penanggulangan Kecurangan Pembayaran Melalui QRIS Yang Dilakukan Oleh Konsumen Dalam Transaksi Elektronik

Penanggulangan kriminal dapat dibagi menjadi dua kategori, yaitu melalui pendekatan hukum pidana (penal) dan pendekatan luar ranah hukum pidana (non-penal). Upaya non-penal mencakup pencegahan tanpa akibat hukum dan pengaruh terhadap perseptif umum tentang kriminal melalui media massa. Diferensiasi utama antara keduanya adalah pendekatan penal bersifat represif dengan memberikan efek jera, sementara pendekatan non-penal lebih bersifat preventif, bertujuan untuk mencegah kejadian sebelum terjadi.⁷⁶

A. Upaya Represif

Setelah terjadi tindak pidana, langkah yang diambil adalah tindakan represif, yang dilaksanakan oleh penegakan hukum, terutama hukum pidana. Tujuan dari hukum pidana adalah menimbulkan efek jera pada pelaku dan mencegah peristiwa serupa terjadi di masa depan. Hukum pidana juga diciptakan untuk melindungi hak asasi manusia individu yang menjadi korban kejahatan dan kepentingan publik secara keseluruhan. Aturan-aturan ini mengatur tindak pidana penipuan, terutama penipuan yang dilakukan melalui internet, yakni:

⁷⁶ Nugroho, Rizka Adi, dan Prihati Yuniarlin. "Pelaksanaan Jual Beli Secara Online Berdasarkan Perspektif Hukum Perdata." *Media of Law and Sharia* 2, No. 2 (2021).

A. Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) mengatur tentang penipuan. Pasal ini menyatakan bahwa seseorang yang dengan sengaja dengan nama palsu atau kehilangan martabat karena melanggar hukum dengan tujuan memperoleh keuntungan bagi dirinya sendiri atau orang lain dengan cara menipu atau membujuk orang lain untuk berhutang, memberikan, atau membatalkan hutang, dapat dihukum dengan penjara maksimal empat tahun.⁷⁷

B. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) tidak secara spesifik mengatur tentang penipuan, namun mengatur tentang timbulnya kerugian dalam transaksi elektronik. Pasal 28 ayat (1) UU ITE juncto pasal 45A ayat (1) UU ITE mengatur tentang sanksi pidana bagi pelanggar, yaitu maksimal 6 tahun penjara atau denda maksimal 1 miliar rupiah.

Langkah melakukan tindakan pelaku penipuan dalam transaksi online dapat dihukum sesuai dengan ketentuan yang tercantum penjatuhan sanksi pidana bagi pelaku penipuan online diatur dalam KUHP dan UU ITE, dan dilakukan melalui mekanisme peradilan pidana. Penerapan hukum pidana sebagai tindakan represif untuk mencegah dan menghentikan kejahatan teknologi, mengingat efek buruk dan kerugian yang timbul dari

⁷⁷ Kitab Undang-Undang Hukum Pidana (KUHP) Pasal 378 tentang Penipuan

kemajuan teknologi informasi yang cepat. Sanksi pidana bertujuan untuk mencegah kerugian yang timbul bagi masyarakat, dengan memberikan hukuman yang dapat membuat pelaku lebih berhati-hati. Kerugian yang diakibatkan oleh penipuan dapat berdampak negatif pada ekonomi korban dan menghambat aktivitas sosial-ekonomi masyarakat.

Hukuman pidana dianggap sesuai bagi pelaku penipuan belanja online yang merugikan korban. Namun, upaya represif melalui proses hukum pidana sering terjadi tidak digunakan dalam kasus penipuan belanja online. Hal ini disebabkan oleh berbagai kendala yang dihadapi oleh pihak kepolisian, meskipun banyak korban yang mengalami kerugian. Seperti yang dialami ketiga pelaku usaha yang mana bukan sekali maupun dua kali mereka merasakan penipuan via QR tersebut tetapi sudah sering sehingga menyulitkan penghasilan mereka.⁷⁸

B. Upaya Preventif / Pencegahan,

Meskipun menguntungkan, transaksi jual-beli online juga dapat memiliki kerugian dan efek negatif yang harus diwaspadai.. Tingginya angka penipuan internet yang beragam metode adalah salah satu efek negatif dari kemajuan sistem jual-beli ini. Jumlah kasus penipuan tidak bisa dianggap kecil karena banyak korban

⁷⁸ Indah, S.C. Maya. *Perlindungan Korban (Suatu Perspektif Viktimologi dan Kriminologi)* (Jakarta, Kencana, 2014).

mengalami kerugian materi yang berkisar antara puluhan ribu dan ratusan juta rupiah. Meskipun ada korban yang signifikan, penipuan online tetap bisa dihindarkan. Salah satu cara untuk pedagang mencegah kecurangan adalah dengan memastikan QR diterima dan mengecek nominal pembelian melalui QR yang telah dipindai oleh konsumen. Selalu bersikap waspada dan hati-hati, serta menguasai pengetahuan yang memadai tentang teknologi untuk melakukan transaksi elektronik dengan aman, sangat penting untuk dilakukan.⁷⁹

Undang-undang yang mengatur terkait perlindungan pelaku usaha memang belum diatur secara eksplisit dan hingga saat ini, belum ada kemajuan yang direncanakan dalam UU No 8 Tahun 1999 tentang perlindungan konsumen. Namun terdapat pada pasal 6 UU No 8 Tahun 1999 yang mengatur mengenai hak bagi pelaku usaha, yang dimana hak tersebut guna untuk melindungi hak bagi pelaku usaha. Hak pelaku usaha tersebut, antara lain :⁸⁰

1. Hak untuk menerima pembayaran sesuai dengan kesepakatan mengenai kondisi dan nilai tukar barang dan/atau jasa yang diperdagangkan.
2. Hak untuk mendapatkan perlindungan hukum dari tindakan konsumen yang tidak beretikad baik

⁷⁹ Jevlin Solim, dkk., “Upaya Penanggulangan Tindak Pidana Penipuan Situs Jual Beli Online di Indonesia” *Jurnal Hukum Samudra Keadilan* 14, No. 1 (2019)

⁸⁰ Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen

3. Hak untuk melakukan pembelaan diri sepatutnya di dalam penyelesaian hukum sengketa konsumen;
4. Hak untuk rehabilitasi nama baik apabila terbukti secara hukum bahwa kerugian konsumen tidak diakibatkan oleh barang dan/atau jasa yang diperdagangkan;
5. Hak-hak yang diatur dalam ketentuan peraturan perundang-undangan lainnya

Hak-hak pelaku usaha yang tercantum pada pasal 6 UU No 9 tahun 1999 tentang Perlindungan konsumen tersebut bagaikan payung yang melindungi hak-hak yang dimiliki pelaku usaha dalam menjalankan kegiatan ekonominya. Hak-hak tersebut ibarat tiang penyangga utama yang menjamin kelancaran usaha dan dapat memberikan kepastian hukum. Pelaku usaha memiliki hak untuk menerima pembayaran sesuai dengan kesepakatan, yang mana hak ini bagaikan jaminan atas hasil jerih payah pelaku usaha dan memastikan bahwa pelaku usaha mendapatkan imbalan yang sepadan dengan nilai barang dan jasa yang ditawarkan. Perlindungan dari konsumen yang tidak beretika baik hadir bagaikan benteng pertahanan, yang mana pelaku usaha berhak terhindar dari tindakan yang merugikan oleh konsumen yang tidak beretika baik, seperti penipuan pembayaran, perusakan barang atau penyebaran ulasan palsu.⁸¹

⁸¹ Undang-Undang Republik Indonesia UU No 9 tahun 1999 tentang Perlindungan konsumen

Pembelaan diri dalam perselisihan konsumen menjadi suara bagi pelaku usaha. Pelaku usaha berhak untuk menjelaskan posisi dan memberikan bukti dalam proses penyelesaian perselisihan. Hal ini dianggap mendapatkan keadilan dan terhindar dari tuduhan yang tidak berdasar. Rehabilitas nama baik bagaikan pemulihan reputasi, jika terbukti bersih dari kesalahan, pelaku usaha berhak mendapatkan reputasi mereka kembali. Hal ini penting untuk menjaga kepercayaan konsumen dan kelangsungan usaha. Hak-hak tambahan yang diatur dalam undang-undang melengkapi perlindungan ini, yang mana pelaku usaha berhak atas informasi yang benar, partisipasi dalam kebijakan dan akses ke penadanaan serta pelatihan. Pasal 6 UU No. 9 tahun 1999 bagaikan perisai ganda yang melindungi hak-hak pelaku usaha dan konsumen. Keseimbangan antara keduanya menjadi kunci terciptanya lingkungan usaha yang mendukung dan memacu pertumbuhan ekonomi yang berkelanjutan.

Penanggulangan Untuk menanggapi kasus penipuan yang dialami oleh Ibu Tiara Dewandari Andre, dan Dwi, diperlukan tindakan yang berbeda dalam penanggulangan serta pencegahannya. Pertama, Ibu Tiara Dewandari dapat menghubungi penyedia layanan pembayaran digital atau lembaga terkait untuk melaporkan kejadian ini dan mencoba mendapatkan bantuan dalam pemulihan dana. Sebagai langkah pencegahan, OJK perlu memberikan pedoman yang jelas kepada pelaku usaha seperti Ibu Tiara Dewandari tentang penggunaan QRIS dan

teknologi *blockchain* serta melaksanakan pelatihan untuk meningkatkan pemahaman dan kewaspadaan terhadap penipuan online.

Blockchain adalah sebuah sistem database terdistribusi yang menggunakan mekanisme kriptografi untuk memastikan keamanan transaksi tanpa memerlukan pihak perantara.⁸² Ini memungkinkan verifikasi transaksi oleh semua pihak dalam jaringan tanpa kemungkinan modifikasi data. Teknologi ini dapat meningkatkan kecepatan, efisiensi, transparansi, dan keamanan transaksi. Studi kasus menunjukkan bahwa penggunaan *blockchain* dalam industri perbankan syariah memiliki potensi untuk meningkatkan keamanan, transparansi, dan efektivitas operasi. Namun, tantangan seperti regulasi yang tepat dan pemahaman yang cukup tentang teknologi ini masih perlu diatasi. Peran lembaga pemerintah, regulator, dan keuangan sangat penting dalam menciptakan kerangka kerja yang mendukung penggunaan *blockchain* dalam transaksi.⁸³

Kedua, Andre yang menjadi korban penipuan juga bisa melaporkan kejadian ini kepada pihak berwenang untuk mendapatkan bantuan dalam proses pemulihan dana yang hilang. Selain itu, pelatihan dan edukasi tentang pentingnya memeriksa notifikasi transaksi secara rutin dapat membantu para karyawan toko seperti Andre untuk menghindari

⁸² Muhammad Bahanan, Muhammad Wahyudi, "Analisis Pengaruh Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Pada Perbankan Syariah." *I'THISOM : Jurnal Ekonomi Syariah* , 2, no. 1 (2023): 46

⁸³ *Ibid*

penipuan di masa depan. Untuk menanggulangi penipuan yang terjadi di situs *e-commerce* Indonesia, langkah-langkah penting telah diambil. Pemerintah telah mengeluarkan berbagai peraturan yang mengatur masalah ini, termasuk Kitab Undang-Undang Hukum Pidana, Undang-Undang Perlindungan Konsumen, dan Undang-Undang tentang Informasi dan Transaksi Elektronik. Selain itu, penting bagi pengguna untuk memverifikasi keamanan situs, menggunakan akun yang asli dengan informasi pribadi yang jelas, dan melakukan pengecekan harga sebelum melakukan transaksi. Badan pengawas seperti Id-SIRTII/CC juga telah dibentuk untuk mengatasi tindak pidana cybercrime. Id-SIRTII/CC (*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center*) adalah garis pertahanan pertama dalam melindungi pengguna internet di Indonesia dari kejahatan dunia maya. Tim ini bertugas menjaga keamanan data orang Indonesia, terutama dari serangan cracker tidak bertanggung jawab yang sering menyerang situs web dan server internet Indonesia.⁸⁴ Melalui edukasi konsumen, pelaporan ke pihak berwenang, dan pelatihan karyawan, diharapkan dapat meningkatkan keamanan transaksi online dan mengurangi insiden penipuan.⁸⁵

⁸⁴ Mira Kania Sabariah, Fiska Mekas Kustiani, "Analisis Data Mart Untuk Virtualisasi Traffic Monitoring Insiden Di ID-SIRTII/CC" *Komputa : Jurnal Ilmiah Komputer dan Informatika* , 2, no 1 (2015): 61

⁸⁵ Jevlin Solim, Mazmur Septian Rumapea, Agung Wijaya, Bella Monica Manurung, Wendy Lionggodinata, "Upaya Penanggulangan Tindak Pidana Penipuan Situs Jual Beli Online Di Indonesia" *Jurnal Hukum Samudra Keadilan* ,14, no. 1 (2019): 106

Ketiga, Dwi perlu melaporkan penipuan yang dialaminya kepada pihak berwenang agar pelaku dapat ditindaklanjuti secara hukum. Sementara itu, sebagai langkah pencegahan, pelaku usaha UMKM, seperti Dwi, perlu diberikan edukasi tentang modus penipuan online yang umum, serta cara-cara untuk memverifikasi transaksi secara efektif guna menghindari kerugian di masa mendatang. Penegakan hukum terhadap penipuan yang terjadi melalui media elektronik memerlukan penerapan kebijakan kriminal, baik dalam bentuk penal maupun non-penal. Kebijakan penal menggunakan hukum pidana, Sementara itu, kebijakan non-penal melibatkan upaya pencegahan sebelum terjadinya tindak pidana meliputi peningkatan kondisi ekonomi masyarakat dan edukasi publik mengenai penggunaan internet yang efektif bersama dengan mengenali karakteristik penipuan melalui media elektronik. Kendala dalam penegakan hukum terhadap tindak pidana penipuan melalui media elektronik meliputi terbatasnya kemampuan dan sumber daya, serta rendahnya kesadaran hukum masyarakat. Untuk mengatasinya, diperlukan kerja sama antara komunitas yang aktif yang memiliki aparat penegak hukum yang demokratis, jelas, dan bertanggung jawab. Polisi perlu bekerja sama dengan lembaga akademik untuk memberikan penyuluhan edukasi kepada masyarakat mengenai efek dari bertransaksi elektronik serta cara mencegah atau menangani tindak pidana penipuan dalam transaksi digital. Selanjutnya, perangkat hukum perlu memperhatikan

perkembangan teknologi informasi dan antisipatif terhadap permasalahan yang muncul. Ini bertujuan untuk memastikan keberlangsungan kondisi pembangunan masyarakat yang merata, sejahtera, dan makmur.⁸⁶ Sebagai contoh, dalam kasus Dwi yang menjadi korban penipuan, langkah pertama adalah melaporkan kejadian tersebut kepada pihak berwenang. Sebagai langkah pencegahan, pelaku usaha UMKM, seperti Dwi, perlu diberikan edukasi tentang modus penipuan online dan cara-cara verifikasi transaksi guna menghindari kerugian di masa mendatang.

Secara umum, penegakan hukum terhadap penipuan online perlu diperkuat melalui kerja sama antara pihak berwenang, lembaga pengawas keuangan, dan pelaku usaha. Selain itu, meningkatkan kesadaran masyarakat tentang modus penipuan yang umum dalam transaksi online serta pengembangan teknologi keamanan seperti *blockchain* juga menjadi langkah penting dalam mengurangi risiko dan dampak dari penipuan online bagi para pelaku usaha dan masyarakat umum.

B. Pengaturan Teknologi *Blockchain* Dalam Upaya Penanggulangan Kecurangan Pembayaran Di Beberapa Negara Maju

Penting untuk dicatat bahwa di Indonesia, metode pembayaran QRIS telah menjadi salah satu pilihan yang populer dalam transaksi elektronik. QRIS

⁸⁶ Agus Kasiyanto, Thon Jerri, "Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Yang Dilakukan Melalui Media Elektronik." *De Facto* Vol 4, no. 2 (2017): 81-82

memanfaatkan kode QR untuk mempermudah pembayaran antara konsumen dan penjual. Namun, berbeda dengan situasi di Indonesia, ada perbedaan pendekatan dalam beberapa negara seperti Amerika Serikat, China, dan Singapura. Di negara-negara tersebut, terdapat tren penggunaan aset kripto (*cryptocurrency*) yang menggunakan teknologi *blockchain* sebagai alat pembayaran yang semakin meningkat.

Teknologi telah mengubah dunia secara fundamental dengan digitalisasi yang tak terelakkan. Digitalisasi sendiri adalah proses konversi atau perubahan dari teknologi yang masih analog menjadi teknologi digital, atau dapat dikatakan sebagai penggunaan teknologi dan data digital dalam meningkatkan kinerja, efisiensi, dan nilai dari aktivitas, fungsi, maupun suatu model bisnis⁸⁷. Digitalisasi juga melibatkan penggunaan teknologi digital untuk merubah cara kita berinteraksi, bekerja, belajar, dan beraktivitas sehari-hari, hal ini menimbulkan peluang baru yang tidak memiliki batas untuk menghubungkan banyak orang di seluruh dunia, memungkinkan berbagi akses terhadap layanan dan informasi secara lengkap dan lebih mudah⁸⁸.

Dalam perkembangan era digital yang terus berkembang dalam masyarakat ini salah satu perkembangan yang menonjol adalah perkembangan teknologi *blockchain*. Teknologi *blockchain* sendiri pertama kali dikenalkan melalui Bitcoin yang sekarang telah menyebar ke berbagai sektor dan industri di seluruh dunia.

⁸⁷ Nono Heryana, Muhammad Fuad, dkk., *UMKM Dalam Digitalisasi Nasional*, (Surabaya: Cendikia Mulia Mandiri, 2023)

⁸⁸ AG. Eka Wenats Wuryanta, "Digitalisasi Masyarakat: Menilik Kekuatan dan Kelemahan Dinamika Era Informasi Digital dan Masyarakat Informasi

Seiring perkembangan Bitcoin, kesadaran mengenai potensi dan manfaat teknologi *blockchain* juga meningkat, para ahli teknologi dan pelaku bisnis mulai menciptakan mata uang digital yang dapat diterapkan dalam aspek kehidupan sehari-hari. Sebagai contoh dalam dunia perbankan, *blockchain* telah membawa pengaruh besar, yakni pada perkembangan kemudahan penggunaan transaksi keuangan maupun pada penyelesaian transaksi lintas batas. Dalam sector logistic, *blockchain* diterapkan untuk menciptakan pencatatan yang aman serta transparan yang bermula dari produsen sampai dengan konsumen terakhir.⁸⁹

Selain itu, di berbagai negara, teknologi *blockchain* juga dimanfaatkan untuk menciptakan identitas digital yang aman dan dapat dipercaya. Pemanfaatan *blockchain* juga telah sampai pada titik dapat meningkatkan layanan publik, seperti dalam pemilihan elektronik dan distribusi bantuan kemanusiaan⁹⁰. Namun, tantangan utama dalam pengembangan teknologi *blockchain* adalah menciptakan regulasi yang mendukung inovasi sambil tetap memperhatikan keamanan dan perlindungan konsumen. Banyak negara dan lembaga internasional masih berupaya mengembangkan kerangka regulasi yang sesuai dengan perkembangan teknologi ini. Kesadaran akan potensi teknologi *blockchain* dan pemahaman yang lebih mendalam tentang cara mengimplementasikannya juga masih perlu ditingkatkan di kalangan

⁸⁹ Tito Wira Eka Suryawijaya, "Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital di Indonesia", *JSKP: Jurnal Studi Kebijakan Publik*, 2, No.1, 2023

⁹⁰ Dimas Agung Pangestu, Skripsi: *Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Syariah*, (Yogyakarta: Universitas Islam Indonesia, 2023)

pengusaha, pembuat kebijakan, dan masyarakat umum.

Dengan dukungan yang semakin meningkat dari pemerintah, lembaga riset, dan pelaku bisnis, teknologi *blockchain* berpotensi untuk terus tumbuh dan berperan penting dalam ekonomi digital global. Dengan investasi yang tepat dalam pendidikan, regulasi yang mendukung inovasi, dan kolaborasi yang kuat antara berbagai pihak, teknologi *blockchain* memiliki potensi besar untuk membawa perubahan positif yang signifikan dalam berbagai aspek kehidupan di seluruh dunia⁹¹.

Sebagai perbandingan dengan negara-negara lain, berikut pengaturan teknologi *blockchain* di beberapa negara maju:

1. Pengaturan *Blockchain* Di Amerika Serikat

Teknologi *blockchain* di Amerika Serikat telah mengalami perubahan yang sangat menarik beberapa tahun terakhir ini. *Blockchain* mulai dikenal melalui Bitcoin yang merupakan mata uang kripto pertama yang menggunakan *blockchain*. Bersama dengan Bitcoin, penggunaan mata uang digital yang terdesentralisasi dengan tidak terikat otoritas sentral bank atau pemerintah mulai diperkenalkan kepada masyarakat luas dan mengalami kesuksesan besar. Kesuksesan tersebut membuat teknologi *blockchain* mulai diminati dan mengalami perkembangan pesat dengan semakin banyaknya pengembang independent maupun perusahaan besar yang mulai mengeksplorasi

⁹¹ *Op.cit.*

potensi yang dimiliki oleh teknologi *blockchain* di luar cakupan mata uang digital. Mereka juga sadar bahwa teknologi ini dapat digunakan dalam berbagai aspek mulai dari aspek kehidupan sehari-hari seperti perawatan kesehatan, identitas digital, rantai pasokan, dll⁹².

Inovasi dalam bidang *blockchain* terus berkembang di Amerika Serikat, mulai banyak perusahaan, lembaga, maupun *startup* yang mengembangkan produk maupun layanan berbasis *blockchain* untuk menciptakan hasil yang lebih efisien, transparan, dan aman⁹³. Selain itu, institusi maupun bank-bank besar juga banyak yang telah melakukan pengujian untuk meningkatkan efisiensi dalam transaksi keuangan.

Di Amerika Serikat sendiri teknologi ini masih relative baru dan terus berkembang sehingga pengaturan hukum mengenai *blockchain* juga masih dalam proses pengembangan, namun terdapat beberapa badan pemerintahan federal atau beberapa negara bagian yang telah memiliki produk hukum sendiri yang mengatur aspek-aspek tertentu dari teknologi *blockchain*, beberapa diantaranya adalah sebagai berikut:

⁹² Ahmed G. Gad, Diana T. Mosa, Laith Abualigah, dan Amr. A. Abohany, "Emerging Trends In Blockchain Technology And Application: A Review And Outlook", *Journal of King Saud University – Computer and Information Sciences*, Vol.34 No.9, 2022

⁹³ Omar Ali, Mustafa Ally, Clutterbuck, dan Yogesh Dwivedi, "The State of Play of Blockchain Technology in The Financial Services Sector: A Systematic Literature Review", *International Journal of Information Management*, Vol.52 102199, 2020

a. Securities and Exchange Commission (SEC)

Securities and Exchange Commission (SEC) merupakan lembaga pengawasan bursa efek di Amerika Serikat. SEC memiliki tugas utama dalam mengendalikan dan memantau industry sekuritas yang berfokus pada perlindungan investor, menjamin keterbukaan informasi di pasar, serta menghindari tindakan penipuan dan manipulasi di pasar⁹⁴.

SEC telah mengeluarkan beberapa panduan dan peraturan mengenai asset kripto yang beroperasi harus dengan cara yang adil dan transparan. Salah satu bagian yang diatur oleh SEC adalah mengenai apakah suatu koin digital dianggap sebagai sekuritas atau tidak, dalam hal ini apabila termasuk dalam sekuritas, SEC mengatur bahwa penerbit harus mendaftarkan kepada SEC dan mematuhi aturan yang berlaku termasuk menyampaikan resiko terkaitnya. Selain itu SEC juga memiliki tanggung jawab atas penegakan hukum atas peratran terkait dengan koin digital dan asset kripto⁹⁵.

b. Commodity Futures Trading Commission (CFTC)

Commodity Futures Trading Commission (CFTC) adalah badan pemerintah federal yang memiliki tanggung jawab atas pengawasan dan regulasi pasar komoditas. CFTC memiliki misi untuk melindungi

⁹⁴ Admin, "Securities and Exchange Commission", *HSB Invest in Time*, Diakses pada 22 April 2024, <https://www.hsb.co.id/glosarium/s/securities-and-exchange-commission>

⁹⁵ Michelle Legge, "SEC & Crypto: How Does The SEC Regulate Crypto?", *Koinly*, 2 Februari 2024, <https://koinly.io/blog/sec-crypto/>

pasar dari tindakan manipulatif, tidak berkeadilan dan tidak transparan, serta memastikan integritas dan stabilitas pasar⁹⁶.

CFTC, dalam perannya sebagai badan pengawas pasar derivatif komoditas, tidak hanya mengatur perdagangan berjangka komoditas seperti minyak, emas, dan pertanian, tetapi juga mengawasi bursa dan pedagang berjangka untuk mencegah manipulasi pasar. Selain itu, mereka memiliki yurisdiksi atas pasar derivatif keuangan, termasuk kontrak berjangka mata uang, suku bunga, dan indeks saham, yang mereka awasi untuk memastikan transparansi dan likuiditas pasar serta melindungi investor dari risiko yang tidak semestinya. Dalam konteks blockchain dan kriptokurensi, CFTC menyatakan bahwa beberapa mata uang kripto dianggap sebagai komoditas dan oleh karena itu tunduk pada regulasi yang relevan, termasuk perdagangan derivatif kripto seperti kontrak berjangka Bitcoin dan opsi mata uang kripto lainnya, dengan fokus pada kepatuhan terhadap peraturan anti-manipulasi dan perlindungan investor⁹⁷.

c. **Financial Crimes Enforcement Network (FinCEN)**

Financial Crimes Enforcement Network (FinCEN) merupakan sebuah lembaga keuangan di bawah Departemen Keuangan AS, memiliki tanggung jawab mengumpulkan, menganalisis, dan

⁹⁶ Agency, "Commodity Futures Trading Commission", *Federal Register*, Diakses pada 22 April 2024, <https://www.federalregister.gov/agencies/commodity-futures-trading-commission>

⁹⁷ Team, "The Commission", *CFTTC: Commodity Futures Trading Commission*, Diakses pada 22 April 2024, <https://www.cftc.gov/About/AboutTheCommission>

membagikan informasi keuangan untuk mendukung penegakan hukum dan kebijakan anti- pencucian uang di seluruh negeri. Sebagai pusat intelijen keuangan nasional, FinCEN memantau sejumlah kejahatan keuangan, termasuk pencucian uang, pendanaan terorisme, dan aktivitas keuangan ilegal lainnya⁹⁸.

Dalam konteks teknologi *blockchain*, FinCEN mengawasi transaksi keuangan yang melibatkan aset kripto dengan tujuan mencegah penyalahgunaan dalam kegiatan keuangan ilegal, termasuk pencucian uang dan pendanaan terorisme. Seiring dengan perkembangan teknologi *blockchain*, FinCEN berperan dalam mengatur dan mengawasi penggunaan mata uang kripto, menerapkan peraturan yang mengharuskan platform pertukaran kripto untuk patuh terhadap prosedur identifikasi pelanggan, melaporkan transaksi yang mencurigakan, dan mematuhi regulasi anti- pencucian uang yang berlaku. Oleh karena itu, peran kunci FinCEN adalah menjaga integritas sistem keuangan Amerika Serikat dan memastikan bahwa teknologi *blockchain* dimanfaatkan dengan bertanggung jawab dalam kegiatan keuangan⁹⁹.

d. Internal Revenue Service (IRS)

Internal Revenue Service (IRS) adalah badan pemerintah federal

⁹⁸ Administrator, “Advisory to Financial Institutions and Real Estate Firms and Professionals”, *Financial Crimes Enforcement Network*, 22 Agustus 2017, Diakses pada 23 April 2024, <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a003>

⁹⁹ *Ibid.*

di Amerika Serikat yang memiliki tugas untuk mengumpulkan pajak dan menegakkan peraturan perpajakan. IRS merupakan bagian dari Departemen Keuangan Amerika Serikat yang memiliki peran penting dalam mengatur sistem perpajakan negara dan memastikan kepatuhan terhadap undang-undang perpajakan yang berlaku¹⁰⁰.

IRS memiliki tugas memastikan transaksi yang melibatkan aset kripto mematuhi peraturan perpajakan yang berlaku. Seiring dengan perkembangan teknologi *blockchain*, IRS harus memastikan bahwa pendapatan dari aktivitas kripto dilaporkan dengan teliti untuk keperluan perpajakan. Selain itu, IRS memiliki kewenangan untuk melakukan audit terhadap transaksi kripto guna memastikan kepatuhan terhadap undang-undang perpajakan yang berlaku¹⁰¹.

e. Regulasi Federal

Beberapa negara bagian di Amerika Serikat memiliki peraturan sendiri mengenai teknologi *blockchain*, sehingga untuk peraturan yang ada belum merata ke seluruh bagian Amerika Serikat. Sebagai contoh pada New York yang memiliki regulasi BitLicense yang merupakan lisensi khusus perusahaan yang beroperasi dalam industry mata uang virtual¹⁰².

¹⁰⁰ Michelle P. Scott, "What's Wrong With the American Tax System", *Investopedia*, 16 Agustus 2023, Diakses pada 23 April 2024, <https://www.investopedia.com/articles/personal-finance/082415/whats-wrong-american-tax-system.asp>

¹⁰¹ Robert A. LeBaube, "9 Assisting Taxpayers in Meeting Their Obligations Under the Law", *IMF eLibrary*, Diakses pada 23 April 2024, [https://www.elibrary.imf.org/configurable/content/book\\$002f9781557753175\\$002fch009.xml?t:ac=book%24002f9781557753175%24002fch009.xml](https://www.elibrary.imf.org/configurable/content/book$002f9781557753175$002fch009.xml?t:ac=book%24002f9781557753175%24002fch009.xml)

¹⁰² Primavera De Filippi, Morshed Mannan, Wessel Reijers, "Blockchain As A Confidence Machine: The Problem Of Trust & Challenges Of Governance", *Technology in Society*, Vol.62

2. Pengaturan *Blockchain* Di China

Teknologi *blockchain* sangat erat kaitannya dengan *cryptocurrency*, sedangkan di China sendiri terdapat larangan aktivitas perdagangan dan penggunaan mata uang kripto, sehingga pengaturan hukumnya menggunakan pendekatan yang sangat ketat terhadap penggunaan *blockchain*. Pada tahun 2017, pemerintah China mengumumkan larangan yang tegas terhadap perdagangan mata uang kripto dan ICO (*Initial Coin Offering*) di wilayahnya. Tindakan ini dilakukan untuk mengontrol spekulasi pasar dan mengurangi risiko keuangan yang terkait dengan mata uang kripto. Selain menetapkan larangan perdagangan mata uang kripto, pemerintah China juga menerbitkan sejumlah regulasi yang mengatur penggunaan teknologi *blockchain* di berbagai sektor ekonomi. Sebagai contoh, pemerintah China menetapkan persyaratan pendaftaran dan perizinan untuk penggunaan *blockchain* dalam industri tertentu seperti keuangan, perbankan, dan *e-commerce*¹⁰³.

Tidak hanya itu, pemerintah China juga telah mengambil langkah untuk meningkatkan kontrol dan pengawasan terhadap pihak pengguna *blockchain*, seperti terhadap penyedia layanan *blockchain*, pemerintah China wajib untuk memantau dan melaporkan aktivitas

101284, 2020

¹⁰³ Jia Wang, Lei Chen, "10 Regulating Smart Contracts and Digital Platforms", *Cambridge University Press*, 25 Oktober 2019, Diakses pada 23 April 2024, <https://www.cambridge.org/core/books/abs/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/regulating-smart-contracts-and-digital-platforms/5CD6E83BF98B5D0F34D62723EC195276>

pengguna dengan lebih ketat. Langkah ini dilakukan untuk mengurangi kemungkinan penyalahgunaan teknologi blockchain untuk tujuan yang ilegal¹⁰⁴.

3. Pengaturan *Blockchain* Di Singapura

Singapura merupakan negara yang sangat mendorong inovasi dalam teknologi *blockchain* dengan mengadopsi pendekatan yang progresif dan menciptakan lingkungan yang kondusif bagi perkembangan teknologinya. Pihak yang paling berperan dalam pengembangan regulasi mengenai teknologi *blockchain* adalah *Monetary Authority of Singapore* (MAS)¹⁰⁵.

MAS telah menerbitkan panduan mengenai penggunaan *blockchain* dan *cryptocurrency* pada 2019 yakni mengenai “*Payment Services Act*” yang mengatur mengenai perlindungan konsumen dalam ruang lingkup keamanan transaksi dengan pembayaran digital. Selain itu, pemerintah juga terus melakukan pengawasan perkembangan teknologi *blockchain* untuk selalu siap siaga melakukan penyesuaian regulasi dengan keadaan perubahan pasar maupun perubahan teknologi.

4. Rekomendasi Pengaturan *Blockchain*

Regulasi *blockchain* di Amerika Serikat, China, Singapura, dan Indonesia menunjukkan pendekatan yang beragam terhadap inovasi

¹⁰⁴ *Ibid.*

¹⁰⁵ Yovianda Arief Pratama, Tesis: *Legalitas Hukum Coin Cryptocurrency Sebagai Alat Pembayaran Di Indonesia*, (Yogyakarta: Universitas Islam Indonesia, 2024)

teknologi tersebut. Amerika Serikat lebih condong pada model yang lebih terbuka dan progresif, memungkinkan perkembangan *blockchain* namun tetap mengawasi aktivitas terkait. Sebaliknya, China mengambil langkah lebih tegas dengan melarang sebagian besar perdagangan mata uang kripto, sambil mendorong pengembangan teknologi *blockchain* demi kepentingan negara. Singapura, sebagai pusat keuangan dan teknologi di Asia, menerapkan pendekatan progresif dengan menciptakan lingkungan yang mendukung perkembangan *blockchain* serta menjaga kepatuhan terhadap regulasi keuangan yang ketat. Di Indonesia, regulasi *blockchain* masih dalam tahap pengembangan, di mana pemerintah sedang mempertimbangkan pendekatan yang seimbang antara inovasi dan perlindungan konsumen, serta kepatuhan terhadap hukum yang berlaku.

Apabila regulasinya dibandingkan, pengaturan hukum di Amerika Serikat, China, dan Singapura terlihat lebih matang dan terstruktur dibandingkan dengan Indonesia. Amerika Serikat dan Singapura memberikan ruang lebih besar bagi inovasi sambil tetap memperhatikan keamanan dan perlindungan konsumen, sedangkan China menerapkan pendekatan yang lebih ketat dengan mengendalikan perdagangan kripto. Di sisi lain, Indonesia masih dalam tahap pengembangan regulasi *blockchain*, namun kesadaran akan pentingnya regulasi yang jelas dan mendukung inovasi semakin

meningkat. Dengan minat yang meningkat dalam pengembangan ekosistem *blockchain*, Indonesia memiliki potensi untuk mengembangkan regulasi yang sesuai dengan kebutuhan lokal sambil memperhatikan prinsip inovasi, keamanan, dan perlindungan konsumen¹⁰⁶.



¹⁰⁶ Amiruddin, Setiadi Yazid, Bayu Anggorojati, dkk., *Tinjauan Strategis Keamanan Siber Indonesia*, (Bogor: Politeknik Siber dan Sandi Negara Press, 2023)