

Between Innovation and Protection: Finding Balance in Blockchain Regulations to Ensure Security and Fairness in Electronic Transactions

[Antara Inovasi dan Perlindungan: Menemukan Keseimbangan Dalam Regulasi Blockchain untuk Menjamin Keamanan dan Keadilan Dalam Transaksi Elektronik]

Alicia Noviandari¹⁾, Mochammad Tanzil Multazam²⁾

¹⁾Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

²⁾Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

*Email Penulis Korespondensi: Tanzilmultazam@umsida.ac.id

Abstract. The research aims to provide recommendations for legal regulation and supervision of blockchain technology as well as legal protection strategies for consumer rights in a more general and comprehensive context. This research uses a normative juridical methods with a statutory approach. The results obtained in this research show that blockchain is decentralized without a central authority to regulate and supervise electronic transactions. The results of this research show that there are no specific regulation governing the comprehensive application of blockchain technology in electronic transactions. The Indonesian government has significant legal authority in handling disputes over electronic transactions in the blockchain ecosystem. Based on ITE Law No. 11/2008, the government is responsible for ensuring that electronic transaction, including blockchain based ones, comply with the principles of legal certainty, prudence and good faith. Article 40 of ITE Law confirms the government's authority to facilitate the use of information technology and protect the public interest from misuse of electronic information. This includes enforcing rules to prevent digital fraud and other intrusions. Additionally, the government may issue additional regulations to address technological developments and dispute resolution, as well as ensure compliance with security and privacy standards.

Keywords- Blockchain, Legal Protection, Electronic Transactions

Abstrak. Penelitian ini bertujuan untuk memberikan saran mengenai pengaturan hukum dan pengawasan teknologi blockchain serta perlindungan hukum terhadap hak konsumen dalam konteks yang lebih luas dan mendalam. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan undang-undang (pendekatan Statute). Temuan dari penelitian ini adalah bahwa blockchain memiliki sifat desentralisasi tanpa otoritas pusat untuk mengatur dan mengawasi transaksi elektronik. Hasil penelitian menunjukkan bahwa belum ada regulasi yang secara khusus mengatur penerapan teknologi blockchain dalam transaksi elektronik secara menyeluruh. Pemerintah Indonesia memiliki kewenangan hukum yang signifikan dalam menangani perselisihan terkait transaksi elektronik di platform blockchain. Menurut Undang-Undang ITE 11/2008, pemerintah memiliki tanggung jawab untuk memastikan bahwa transaksi elektronik, termasuk yang menggunakan teknologi blockchain, mematuhi prinsip-prinsip kepastian hukum, kehatian, dan itikad baik. Pasal 40 Undang-Undang ITE menegaskan bahwa pemerintah memiliki otoritas untuk mendukung penggunaan teknologi informasi serta melindungi kepentingan umum dari penyalahgunaan informasi elektronik, termasuk dalam memberlakukan aturan guna mencegah tindakan penipuan digital dan gangguan lainnya. Pemerintah juga dapat menerbitkan peraturan tambahan untuk mengontrol kemajuan teknologi dan menyelesaikan konflik serta memastikan kepatuhan terhadap standar keamanan dan privasi.

Kata Kunci- Blockchain, Perlindungan hukum, Transaksi elektronik

I. PENDAHULUAN

Saat ini teknologi dan informasi mengalami perkembangan yang cukup signifikan. Hal ini mengubah banyak aspek kehidupan masyarakat. Khususnya dalam sektor perdagangan dengan adanya internet, yang mendukung e-commerce dan menciptakan lingkungan tanpa batas ruang dan waktu. Pertumbuhan teknologi yang terus berlanjut telah menghadirkan model-model baru dalam kegiatan perdagangan elektronik (e-commerce) salah satunya Blockchain [1]. Blockchain, yang awalnya dikenal sebagai platform penyelenggara keuangan digital terutama dalam sistem cryptocurrency, telah mengalami perkembangan yang signifikan sejak tahun 2014. Teknologi ini tidak lagi terbatas pada cryptocurrency saja, tetapi telah memunculkan inovasi baru yang berpengaruh luas terhadap berbagai

aspek kehidupan manusia. Saat ini, blockchain telah terintegrasi ke dalam berbagai sektor inovasi teknologi, mencerminkan transformasi yang mendalam dalam berbagai layanan teknologi di seluruh dunia [2].

Berdasarkan pada hasil laporan Komisi Uni Eropa, penggunaan blockchain telah menunjukkan tren signifikan di berbagai negara dengan penetrasi yang luas di sektor-sektor seperti keuangan, teknologi, kesehatan, energi, dan industri material. Sekitar 600 perusahaan mengadopsi blockchain dalam sektor keuangan, 500 perusahaan berperan sebagai pengembang teknologi blockchain, dan 200 perusahaan lainnya mengembangkan layanan konsumen serta mengaplikasikan teknologi ini dalam sektor-sektor lainnya [3]. Perkembangan ini menunjukkan bahwa blockchain bukan hanya sekadar teknologi baru, tetapi sebuah inovasi yang transformatif dengan potensi untuk merubah cara interaksi antara entitas bisnis dan pemerintah. Dengan terus berkembangnya inovasi ini, baik dari segi kuantitas maupun kualitas, teknologi blockchain mampu mengubah paradigma kehidupan manusia menuju arah yang diinginkan. Namun, untuk memanfaatkan potensi penuh dari teknologi blockchain, penting untuk memiliki tata kelola yang efektif dan regulasi yang tepat [4]. Aturan operasional yang sudah ada, seperti Peraturan POJK Nomor 37/POJK.04/2018 tentang Layanan urun dana melalui penawaran saham berbasis teknologi informasi (Equity Crowdfunding), merupakan contoh bagaimana regulasi dapat menciptakan kondisi yang kondusif untuk adopsi dan pemanfaatan blockchain dalam sektor keuangan.

Kemunculan blockchain telah membawa era baru dalam reformasi digital dan berpengaruh besar terhadap berbagai sektor inovasi teknologi saat ini. Potensi dan manfaat yang ditawarkan oleh teknologi ini akan menjadi kenyataan jika didukung oleh tata kelola yang baik dan regulasi yang memadai untuk menciptakan lingkungan yang kondusif bagi pertumbuhan dan adopsi blockchain di seluruh dunia. Mekanisme bertransaksi aset kripto dilaksanakan dengan jaringan yang bernama Blockchain. Blockchain ataupun teknologi blockchain menjadi suatu sistem transaksi dan tata kelolanya dari sebuah data digital yang seluruh pengguna bergabung pada satu consensus maupun buku besar digital ternama. Peminat investasi aset kripto yang semakin pesat menjadi sebuah objek investasi, serta keuntungan yang tinggi akan didapatkan dari investasi, mengakibatkan masyarakat Indonesia mulai tergiurkan dalam melakukan investasi, maka pengaruh meningkatnya pengguna aset kripto ini apabila terlihat dari aspek hukum Indonesia dapat mengakibatkan berbagai model masalah untuk bertransaksi digital aset kripto yang memposisikan investor aset kripto yang paling dirugikan dengan masalah itu. Salah satunya bentuk potensi pelanggaran di bidang aset kripto ialah pelanggaran memanipulasi harga ataupun praktik monkey business [5]. Namun saat ini belum adanya regulasi khusus yang mengatur tentang penerapan teknologi blockchain dalam transaksi elektronik secara komprehensif. Blockchain hanya diakui sebagai layanan pendukung dalam urun dana berbasis teknologi informasi, terutama dalam konteks keuangan. Padahal, di Indonesia, meskipun penggunaan blockchain masih terbatas, teknologi ini telah mulai digunakan dalam berbagai bidang di luar sektor keuangan [6]. Kondisi ini tidak selaras dengan prinsip-prinsip penggunaan teknologi secara makro menurut hukum positif di Indonesia, di mana setiap penggunaan teknologi harus tunduk pada prinsip kepastian hukum.

Di Indonesia, pengakuan hukum terhadap teknologi menjadi penting untuk memastikan bahwa setiap penggunaan teknologi, termasuk blockchain, mendapat landasan yang jelas dari segi regulasi. Saat ini, ada kebutuhan untuk mengadaptasi regulasi yang ada agar dapat memfasilitasi penggunaan blockchain secara lebih luas dan efektif. Ini penting mengingat bahwa blockchain memiliki potensi besar untuk mengatasi berbagai tantangan di sektor publik dan privat, terutama mengingat kondisi sosial dan budaya masyarakat Indonesia yang sering kali ditandai dengan rendahnya tingkat transparansi. Kepemilikan akan cryptocurrency yakni kepemilikan virtual currency yang paling mempunyai risiko dan banyak terjadi spekulasi sebab nilai perdagangan paling fluktuatif yaitu kenaikan dan penurunan tercepat serta rawannya menjadi target kejahatan dunia maya (Cybercrime) misalnya penipuan, pencucian uang dan pendanaan teroris yang bisa membawa kerugian masyarakat. Tetapi sampai sekarang belum adanya ketetapan untuk aturan perundungan yang dengan khususnya memberi perlindungan hukum pada keamanan asset kripto investor maka mengakibatkan masalah untuk masyarakat yang punya keinginan maupun yang telah menginvestasikan pada crypto untuk investasinya pada kejahatan dunia maya itu [7].

Maka di Indonesia ini juga dihadapkan pada tuntutan dari komunitas internasional terkait pengembangan teknologi blockchain. Ada tekanan untuk mengikuti tren internasional yang semakin mengintegrasikan inovasi blockchain dalam berbagai aspek teknologi. Posisi Indonesia dalam menghadapi ini dapat menjadi pelopor atau sekadar mengikuti arus, tergantung pada kebijakan yang diambil dalam mengatur dan memanfaatkan blockchain [8]. Untuk mencapai integrasi yang berhasil antara kemajuan teknologi dan regulasi, Adaptasi regulasi juga menjadi krusial untuk mempertimbangkan cara blockchain dapat berfungsi secara efektif dalam konteks hukum yang berlaku. Mengingat bahwa blockchain memungkinkan aktivitas yang dilakukan secara otomatis dan terdistribusi dalam jaringan komputasi, penting untuk memikirkan bagaimana aturan hukum dapat diterapkan dan dijalankan di dalam jaringan tersebut. Di Indonesia cryptocurrency terus mengalami perkembangan dan banyak mengakibatkan kontroversi pada masyarakat atas kemunculannya. Berdasar persepsi pemerintah, mempergunakan kerahasiaan bisa memperlemah kedaulatan pemerintah. Sebab rupiah menjadi lambang kedaulatan negara, sehingga pada UU Mata Uang No. 7/ 2011 mengemukakan jika lambang kedaulatan negara salah satunya ialah mata uang.

Dalam UU Mata Uang No. 7/ 2011, menggunakan uang tunai menjadi alat pembayaran dilarang di Indonesia. Selain itu, aturan ketetapan mengenai perdagangan aset (aset kripto) di pasar berjangka No. 8/ 2021. Perlindungan hukum pada konsumen untuk membeli aset crypto dengan transaksi elektronik di indonesia belum diaturkan khusus, tetapi terdapat berbagai aturan yang relevan : 1.) UU Perlindungan Konsumen (UU PK): Walaupun tidak dengan spesifik mengaturkan aset kripto, UU PK memberi dasarnya perlindungan untuk konsumen ketika bertransaksi elektronik. Konsumen punya hak dalam mendapat informasi yang lengkap dan akurat sebelum melakukan pembelian. 2.) UU Informasi dan Transaksi Elektronik (UU ITE): UU ITE mengaturkan mengenai transaksi elektronik dan memberi perlindungan untuk penggunanya. Untuk konsumen yang melaksanakan bertransaksi aset kripto dengan platform elektronik, UU ITE memberi penegasan penting untuk penyediaan data informasi yang lengkap dan akurat. 3.) Aturan Pemerintah mengenai Penyelenggaraan Sistem dan Transaksi Elektronik dalam Perbappehti No. 8/ 2021 tentang : Aturan ini memberi amanatnya dalam pembentukan bursa kripto menjadi bagian dari usaha menguatkan perlindungan konsumen. Selain itu, Perbappehti No. 8/2021 juga mengaturkan mengenai terselesainya persengketaan dengan litigasi ataupun non-litigasi apabila kerugian yang ditimbulkan dari membeli aset crypto pada perdagangan elektronik [9]. Indonesia perlu segera mempersiapkan diri dengan mengadopsi pendekatan yang proaktif dalam mengatur blockchain, bukan hanya menunggu negara lain untuk menyediakan layanan blockchain untuk Indonesia [10]. Ini akan membantu Indonesia untuk tetap relevan dalam komunitas internasional dan memastikan bahwa teknologi blockchain dapat memberikan manfaat maksimal bagi pembangunan dan kemajuan di dalam negeri [11].

Penelitian terdahulu sangat berperan penting sebagai acuan dalam penelitian yang akan dilakukan peneliti saat ini. Penelitian pertama oleh Eureka Inola Kadly, Sinta Dewi Rosadi, Elisatris Gultom dengan judul "Keabsahan blockchain-smart contract dalam transaksi elektronik: Indonesia, Amerika Dan Singapura". Penelitian ini bertujuan untuk membandingkan keabsahan penggunaan blockchain dan smart contract dalam transaksi elektronik di Indonesia, Amerika Serikat, dan Singapura. Penelitian ini juga ingin menganalisis perbedaan pendekatan hukum ketiga negara terhadap teknologi ini. Hasil penelitian menunjukkan bahwa ketiga negara memiliki pendekatan yang berbeda terhadap pengaturan blockchain dan smart contract. Indonesia, Amerika Serikat, dan Singapura memiliki regulasi yang berbeda-beda dalam mengakomodasi teknologi ini dalam transaksi elektronik. Penelitian ini memberikan wawasan tentang tantangan dan potensi pengembangan regulasi di Indonesia terkait penggunaan blockchain dan smart contract. Penelitian kedua oleh Satria Muhammad Nur Lase, Aisyah Adinda, Rizkia Diffa Yuliantika dengan judul "Kerangka hukum teknologi blockchain berdasarkan hukum siber di Indonesia". Penelitian ini bertujuan untuk menyusun kerangka hukum yang mengatur teknologi blockchain berdasarkan hukum siber di Indonesia. Penelitian ini menghasilkan pengaturan terkait kerangka hukum teknologi blockchain berdasarkan hukum siber di Indonesia. Hasilnya mencakup rekomendasi terhadap aspek-aspek hukum yang harus diatur untuk mendukung pertumbuhan ekosistem blockchain. Penelitian ketiga oleh Tanzil Multazam (2024) dengan Judul "*Securing Blockchain Enterprises : Legal Due Diligence Amidst Rising Cyber Threats*". Penelitian ini punya tujuan dalam pemahaman kerentanan yang dihadapi bagi perusahaan yang beroperasikan bisnis blockchain dengan basis token dan peran prosedur pengujian tuntas dan legal untuk memitigasikan risiko itu. Hasil penelitian ini menyoroti bahwa serangan Infrastruktur, terutama melalui Private Key Compromise, merupakan serangan yang paling menimbulkan dampak. Hal ini menyebabkan kerugian lebih dari 800 juta dolar antara tahun 2020 dan 2023. Hal ini memerlukan hukum yang komprehensif dan dapat disesuaikan, strategi uji tuntas yang berfokus pada kerangka hukum yurisdiksi, ketentuan penggunaan platform, kepatuhan terhadap peraturan, dan potensi masalah hukum. Studi ini menegaskan pentingnya penelitian lebih lanjut untuk mengevaluasi dan meningkatkan efektivitas langkah-langkah ini dalam mengatasi tantangan unik teknologi blockchain, yang sangat penting untuk meningkatkan ketahanan dan keberlanjutan perusahaan-perusahaan blockchain, sehingga meningkatkan kepercayaan global dalam bidang yang sedang berkembang ini [12]. Penelitian keempat oleh Mohammad Tanzil Multazam (2021) dengan judul "*Unleashing the Potential of DeFi: A Comprehensive Guide to Maximizing Rewards While Mitigating Risks*". Penelitian ini menganalisis potensi keuntungan dan risiko keuangan dengan desentralisasi ataupun DeFi. Tujuan penelitian ini agar mempunyai pemahaman dalam industri tersebut untuk pembuatan keputusan investasi yang tepat sehingga investor dapat lebih baik memahami industri tersebut. Hasil membuktikan jika DeFi tidak diatur oleh pemerintah (industri anonim dan independen) karena berbeda dengan keuangan tradisional. Dimana DeFi dihasilkan dari pemodal ventura dan protokol dalam bermain peranan penting untuk memperoleh pendapatan pada industri. Investor dilarang berinvestasi seluruhnya dalam bidang ini sebab mitigasi risiko sangat penting untuk mencapai hasil yang tinggi serta beresiko minimal [13]. Penelitian kelima oleh Regita et al (2023) dengan judul "*Is It Legal to Provide Liquidity on the Vexanium Decentralized Exchange in Indonesia?*". Penelitian ini bertujuan untuk menilai keamanan hukum penyedia likuiditas pada Vexanium, blockchain publik pertama di Indonesia. Penelitian ini menganalisis peraturan perundang-undangan terkait blockchain di Indonesia ini melibatkan pemeriksaan awal terhadap proses penyediaan likuiditas. Studi ini menemukan bahwa platform pertukaran terdesentralisasi pada blockchain Vexanium masih harus memenuhi kriteria sebagai elektronik sistem yang mengikuti peraturan perundang-undangan. Selain itu, tidak adanya

informasi yang jelas mengenai pihak-pihak dalam platform membuat kontrak penyediaan likuiditas menjadi batal. Penelitian ini dapat dimanfaatkan bagi pengembang platform di blockchain Vexanium untuk lebih memperhatikan aspek hukum dalam pembuatan platform [14].

Maka terdapat perbedaan antara penelitian terdahulu dengan penelitian yang dilakukan peneliti saat ini bahwa penelitian terdahulu fokus membahas pengaturan blockchain dan smart contract berdasarkan hukum siber di indonesia dan membandingkan antara 3 negara. Sedangkan penelitian saat ini berfokus pada belum adanya regulasi khusus yang mengatur tentang penerapan teknologi blockchain dalam transaksi elektronik secara komprehensif. Hal ini dapat menimbulkan ketidakpastian hukum serta celah dalam proses transaksi, sengketa, dan penegakan hukum. Blockchain bersifat desentralisasi, tanpa otoritas pusat untuk mengatur serta mengawasi transaksi. Hal ini menyulitkan penegakan hukum dan perlindungan konsumen dalam kasus penipuan atau pelanggaran lainnya. Penelitian ini bertujuan memberikan rekomendasi untuk pengaturan hukum dan pengawasan teknologi blockchain serta strategi perlindungan hukum terhadap hak konsumen dalam konteks yang lebih umum dan komprehensif. Maka dapat dirumuskan masalah yaitu : "Apakah Pemerintah Indonesia memiliki kewenangan hukum jika terjadi sengketa pada transaksi elektronik di ekosistem blockchain?".

II. METODE

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan (*Statute approach*). Metode ini digunakan untuk menganalisis menganalisis peraturan dan doktrin hukum terkait teknologi blockchain, dengan fokus pada ketidakpastian hukum dan tantangan desentralisasi teknologi tersebut [15]. Penelitian melibatkan studi dokumen untuk mengumpulkan dan menilai peraturan yang ada, literatur hukum, serta kebijakan terkait, serta analisis kasus hukum untuk menilai penerapan norma hukum [16]. Terdapat 2 bahan hukum yang digunakan dalam penelitian ini yaitu bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer yang digunakan diantaranya UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, UU ITE No. 11/2008, UU 10/2011 perubahan atas UU 10 tahun 2011 tentang Perdagangan berjangka komoditi (PBK), Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan sistem dan transaksi elektronik, Peraturan Bappebti No. 5 Tahun 2019, Peraturan Bank Indonesia terkait penyelenggaraan teknologi finansial 19/12/PBI tahun 2017. Berikutnya, bahan hukum sekunder yang dipergunakan antara lain Buku-buku hukum, artikel, jurnal, website dan lainnya yang relevan dengan topik penelitian. Analisis data yang dilakukan dalam penelitian ini dengan penalaran deduktif berarti pendekatan logis dimana penelitian ini melangkah dari ide-ide umum ke kesimpulan yang khusus.

III. HASIL DAN PEMBAHASAN

A. Pengaturan Hukum Blockchain dalam Transaksi Elektronik

Menurut Bahga dan Madisetti bahwa blockchain adalah sebuah teknologi di mana transaksi dicatat secara andal tanpa memerlukan pihak ketiga sebagai penjamin. Dalam sistem ini, setiap pengguna berperan dalam memverifikasi informasi terkait transaksi secara kolektif. Ini berarti bahwa verifikasi transaksi dilakukan secara terdesentralisasi oleh seluruh peserta jaringan, setiap pihak untuk mengecek dan memastikan keabsahan data yang dicatat. Dengan demikian, teknologi blockchain menghilangkan kebutuhan akan entitas pengawas eksternal dan memastikan keakuratan serta keamanan data melalui konsensus bersama dari semua pengguna yang terlibat.

Blockchain dapat dipahami sebagai sebuah sistem yang membantu individu di seluruh dunia untuk berbagi berbagai jenis informasi. Ini mencakup segala hal mulai dari transaksi keuangan menggunakan mata uang kripto, pengiriman surat berharga, hingga pertukaran data kesehatan dan informasi penting lainnya. Teknologi ini sering dipromosikan karena kemampuannya menyediakan komputasi 'tanpa kepercayaan' (trustless), yang berguna dalam penyimpanan transaksi dengan cara yang tidak dapat diubah, transparan, dan aman.

Blockchain menjamin bahwa transaksi tidak dapat dimanipulasi, baik sebelum maupun sesudah dilakukan, dan mencegah terjadinya transaksi ganda dengan memastikan integritas urutan dan konten transaksi. Kelebihan utama dari blockchain adalah kemampuannya untuk menghilangkan perantara dalam proses transaksi, yang berarti pengguna dapat melakukan transaksi yang aman dan terpercaya tanpa perlu terhubung dengan lembaga tradisional seperti bank, bahkan ketika berinteraksi dengan pihak yang tidak dikenal atau anonim. Maka penting adanya pengaturan hukum blockchain dalam transaksi elektronik untuk memastikan kejelasan, perlindungan, dan keadilan dalam transaksi digital. Regulasi yang jelas membantu mencegah penipuan, melindungi hak-hak pengguna, dan memastikan kepatuhan terhadap standar keamanan dan privasi. Ini juga mendukung kepastian hukum bagi para pelaku bisnis dan investor, memfasilitasi adopsi teknologi secara lebih luas dan aman. Berikut beberapa aturan hukum yang mengatur terkait blockchain dalam transaksi elektronik yaitu Pasal 1 angka 2 UU ITE No. 11 Tahun 2008 mendefinisikan transaksi elektronik sebagai tindakan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, atau media elektronik lainnya. Pasal 3 menekankan bahwa pemanfaatan teknologi informasi dan transaksi elektronik harus

mengikuti prinsip-prinsip seperti kepastian hukum, manfaat, kehati-hatian, itikad baik, serta kebebasan dalam memilih teknologi atau netral teknologi. Sejalan dengan pengaturan yang ada dalam Peraturan Pemerintah 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pasal 1 angka 2 menjelaskan bahwa transaksi elektronik merupakan tindakan hukum yang dilakukan dengan memanfaatkan komputer, jaringan komputer, atau media elektronik lainnya. Sementara itu, Pasal 1 angka 16 mendefinisikan penyelenggaraan transaksi elektronik sebagai serangkaian aktivitas transaksi elektronik yang dilaksanakan oleh Pengirim dan Penerima dengan menggunakan sistem elektronik.

Berikutnya, UU 10/2011 perubahan atas UU 10 tahun 2011 tentang PBK Komoditi digital atau kripto yang berasal dari sistem blockchain dapat dianggap sebagai hak atau kepentingan, sehingga termasuk dalam kategori komoditi [17]. Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial. Aturan ini tidak secara spesifik mengatur blockchain, namun mencakup penggunaan blockchain sebagai platform dalam teknologi finansial, khususnya sistem pembayaran. Pasal 3 Ayat (1) Huruf a menetapkan bahwa sistem pembayaran meliputi otorisasi, kliring, penyelesaian akhir, dan pelaksanaan pembayaran. Dalam konteks ini, teknologi finansial dalam kategori sistem pembayaran mencakup penggunaan teknologi seperti blockchain atau distributed ledger. Teknologi ini digunakan untuk berbagai aplikasi, termasuk transfer dana, uang elektronik, dompet elektronik, dan pembayaran melalui perangkat mobile. Penggunaan teknologi ini dapat meningkatkan efisiensi dan keamanan dalam proses pembayaran dengan menyediakan cara yang lebih terdesentralisasi dan transparan untuk memproses transaksi.

B. Perlindungan Hak Konsumen dalam Menyelesaikan Sengketa pada Transaksi Blockchain

Berdasarkan UU Perlindungan konsumen 8/1999 pasal 1 angka 1 bahwa Perlindungan hak konsumen adalah upaya yang dilakukan untuk memastikan kepastian hukum dan memberikan perlindungan kepada konsumen [18]. Perlindungan hak konsumen dalam menyelesaikan sengketa pada transaksi blockchain di Indonesia melibatkan berbagai regulasi dan undang-undang yang dirancang untuk menjamin keadilan dan keamanan dalam transaksi digital. Berikut adalah penjelasan mengenai beberapa poin penting dalam konteks ini:

1. UU Perlindungan Konsumen 8/1999

UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen adalah landasan hukum utama untuk melindungi hak-hak konsumen di Indonesia. Pasal 2 menyatakan bahwa perlindungan konsumen didasarkan pada prinsip manfaat, keadilan, keseimbangan, keamanan dan keselamatan konsumen, serta kepastian hukum.

Berdasarkan pasal 3 perlindungan konsumen bertujuan untuk “Meningkatkan kesadaran, kemampuan, dan kemandirian konsumen agar dapat melindungi diri mereka sendiri, Mengangkat harkat dan martabat konsumen dengan mencegah dampak negatif dari penggunaan barang atau jasa, Memberdayakan konsumen dalam memilih, menentukan, dan menuntut hak-hak mereka, Menciptakan sistem perlindungan konsumen yang memberikan kepastian hukum, keterbukaan informasi, dan akses untuk memperoleh informasi, Meningkatkan kesadaran pelaku usaha tentang pentingnya perlindungan konsumen sehingga mereka bersikap jujur dan bertanggung jawab, Meningkatkan kualitas barang dan jasa untuk memastikan keberlangsungan usaha serta kesehatan, kenyamanan, keamanan, dan keselamatan konsumen”.

Menurut Pasal 4, hak-hak konsumen meliputi Hak atas kenyamanan, keamanan, dan keselamatan saat menggunakan barang atau jasa, Hak untuk memilih dan menerima barang atau jasa sesuai dengan nilai tukar, kondisi, dan jaminan yang dijanjikan, Hak atas informasi yang akurat, jelas, dan jujur mengenai barang atau jasa, Hak untuk menyampaikan pendapat dan keluhan mengenai barang atau jasa yang digunakan, Hak untuk mendapatkan advokasi, perlindungan, dan penyelesaian sengketa secara layak, Hak untuk menerima pembinaan dan pendidikan konsumen, Hak untuk diperlakukan dengan benar, jujur, dan tanpa diskriminasi, Hak untuk menerima kompensasi, ganti rugi, atau penggantian jika barang atau jasa tidak sesuai dengan perjanjian atau standar yang ditetapkan, Hak-hak lain yang diatur dalam peraturan perundang-undangan lainnya”.

Undang-undang ini memberikan perlindungan dalam berbagai jenis transaksi, termasuk yang dilakukan secara digital melalui blockchain. UU Perlindungan Konsumen mengatur hak-hak dasar konsumen seperti hak atas informasi yang jelas mengenai barang dan jasa yang dibeli, hak untuk mendapatkan barang dan jasa yang sesuai dengan perjanjian, serta hak untuk mendapatkan kompensasi jika terjadi kerugian. Dalam konteks blockchain, di mana transaksi sering kali melibatkan aset digital seperti cryptocurrency, perlindungan ini mencakup hak konsumen untuk mendapatkan transparansi mengenai informasi transaksi dan perlindungan dari praktik penipuan atau penyalahgunaan. Oleh karena itu, meskipun teknologi blockchain adalah hal baru, prinsip perlindungan konsumen tetap berlaku.

2. UU ITE No.11/2008

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 adalah regulasi penting yang mengatur aktivitas e-commerce di Indonesia. UU ITE mencakup berbagai aspek transaksi digital, termasuk yang melibatkan blockchain. UU ini memberikan dasar hukum untuk penyelenggaraan transaksi elektronik, pengaturan

mengenai keamanan dan integritas data, serta perlindungan terhadap aktivitas penipuan dan kejahatan siber. Pasal 3 menetapkan bahwa penggunaan Teknologi Informasi dan Transaksi Elektronik harus mengikuti prinsip kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi.

Pasal 17 menyebutkan bahwa transaksi elektronik dapat dilakukan baik dalam konteks publik maupun privat. Selain itu, para pihak yang terlibat dalam transaksi elektronik harus bertindak dengan itikad baik dalam semua interaksi dan pertukaran informasi atau dokumen elektronik selama proses transaksi. UU ITE mendukung perlindungan konsumen dengan menetapkan standar untuk penyelenggaraan transaksi elektronik dan menetapkan kewajiban bagi pihak-pihak yang terlibat dalam transaksi digital untuk bertindak dengan itikad baik dan menjaga kerahasiaan serta integritas data.

3. Peraturan Bank Indonesia (PBI)

Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial Pasal 3 Ayat (1) mengatur bahwa sistem pembayaran mencakup proses otorisasi, kliring, penyelesaian akhir, dan pelaksanaan pembayaran. Dalam konteks ini, teknologi finansial dalam kategori sistem pembayaran melibatkan penerapan teknologi seperti blockchain atau distributed ledger. Contoh penerapan teknologi ini termasuk dalam sistem transfer dana, uang elektronik, dompet elektronik, dan pembayaran mobile [19]. Teknologi blockchain dapat digunakan untuk meningkatkan efisiensi dan keamanan proses pembayaran dengan menyediakan platform yang terdesentralisasi dan transparan, yang mendukung berbagai jenis transaksi digital secara lebih efektif. PBI ini mengatur bagaimana teknologi finansial, termasuk yang berbasis blockchain, dapat digunakan untuk pemrosesan transaksi pembayaran. PBI memastikan bahwa penyelenggaraan transaksi menggunakan teknologi seperti blockchain harus mematuhi standar keamanan dan transparansi yang ditetapkan oleh Bank Indonesia. Ini penting untuk melindungi konsumen dari risiko yang timbul dari penggunaan teknologi baru dalam transaksi finansial.

Pasal 22 Peraturan Bappebi No. 5 Tahun 2019 mengatur penyelesaian sengketa dalam Pasar Fisik Aset Kripto sebagai berikut: "Pihak-pihak yang berselisih harus terlebih dahulu menyelesaikan sengketa melalui musyawarah sesuai batas waktu yang ditentukan dalam perjanjian. Jika musyawarah gagal, sengketa dapat diselesaikan melalui mekanisme yang disediakan oleh Bursa Berjangka sesuai peraturan yang berlaku. Jika penyelesaian melalui Bursa juga tidak memadai, pihak-pihak dapat memilih untuk menyelesaikan sengketa melalui Badan Arbitrase Perdagangan Berjangka Komoditi (BAKTI) atau Pengadilan Negeri, sesuai forum yang ditetapkan dalam perjanjian".

Musyawarah adalah langkah awal yang diutamakan untuk menyelesaikan sengketa secara damai antara pihak-pihak yang terlibat. Jika musyawarah tidak berhasil, pihak-pihak dapat membawa sengketa ke BAKTI untuk penyelesaian melalui arbitrase. Sebagai alternatif, sengketa juga dapat diajukan ke Pengadilan Negeri untuk penyelesaian hukum formal. Dengan adanya berbagai undang-undang dan peraturan ini, Indonesia berupaya untuk memberikan perlindungan yang komprehensif bagi konsumen dan investor dalam transaksi blockchain, memastikan bahwa mereka dapat menyelesaikan sengketa dengan cara yang adil dan sesuai dengan ketentuan hukum yang berlaku.

C. Kewenangan Hukum Pemerintah Indonesia jika terjadi sengketa pada transaksi elektronik di ekosistem blockchain

Menurut Malayu S.P. Hasibuan, wewenang merupakan kekuasaan yang sah dan legal yang dimiliki oleh individu untuk mengatur atau memerintah orang lain, serta untuk melakukan atau tidak melakukan tindakan tertentu. Dalam konteks pemerintahan, kewenangan mengacu pada hak dan kekuasaan yang dimiliki oleh pemerintah untuk menetapkan dan mengambil keputusan kebijakan dalam rangka pelaksanaan fungsi pemerintahan. Kewenangan ini meliputi hak untuk menentukan arah dan tindakan yang akan diambil dalam berbagai aspek penyelenggaraan negara, baik dalam hal administrasi, peraturan, maupun pelaksanaan kebijakan. Dengan kata lain, kewenangan pemerintah adalah otoritas resmi yang diberikan untuk membuat keputusan, menetapkan peraturan, dan mengatur pelaksanaan kebijakan yang bertujuan untuk menjalankan tugas-tugas pemerintahan secara efektif. Kekuasaan ini harus digunakan sesuai dengan hukum yang berlaku dan bertanggung jawab terhadap publik, guna memastikan bahwa semua tindakan dan kebijakan yang diambil memenuhi prinsip keadilan dan kepentingan umum.

Menurut Pasal 1 angka 2 UU ITE No. 11 Tahun 2008, transaksi elektronik adalah tindakan hukum yang dilakukan melalui komputer, jaringan komputer, atau media elektronik lainnya. Pasal 3 mengatur bahwa pemanfaatan teknologi informasi dan transaksi elektronik harus mematuhi prinsip kepastian hukum, manfaat, kehati-hatian, itikad baik, serta kebebasan memilih teknologi atau netral teknologi. Pasal 4 UU ITE menguraikan "Tujuan pemanfaatan teknologi informasi dan transaksi elektronik, yang mencakup meningkatkan kecerdasan masyarakat, mengembangkan ekonomi nasional, meningkatkan pelayanan publik, memberikan kesempatan bagi individu untuk mengembangkan keterampilan teknologi, serta menjamin rasa aman dan keadilan bagi pengguna dan penyelenggara". Tujuan ini memberikan landasan bagi kebijakan dan regulasi yang mengatur penyelesaian sengketa dengan fokus pada perlindungan hak-hak konsumen dan kepentingan publik. Pasal 17 menyebutkan bahwa "Transaksi elektronik dapat

dilakukan baik dalam konteks publik maupun privat. Selama transaksi berlangsung, semua pihak yang terlibat harus bertindak dengan itikad baik dalam interaksi serta pertukaran informasi dan dokumen elektronik. Aturan lebih lanjut mengenai penyelenggaraan transaksi elektronik diatur oleh peraturan pemerintah”.

Berikutnya, Pada Pasal 39 ayat (3) dalam Peraturan Pemerintah 71/2019 menetapkan “Prinsip-prinsip pengendalian dan pengamanan data pengguna serta transaksi elektronik sebagai berikut yaitu kerahasiaan, integritas, ketersediaan, keautentikan, otorisasi, dan kenirsangkalan”. Berikutnya pada pasal 41 ayat 2 Peraturan Pemerintah 71/2019 menyatakan bahwa “Penyelenggaraan transaksi elektronik dapat dilakukan baik di sektor publik maupun privat. Dalam sektor publik, kegiatan ini mencakup: Instansi, institusi yang ditunjuk oleh Instansi, antar-Instansi, antar-institusi yang ditunjuk, antara Instansi dengan institusi yang ditunjuk, dan antara Instansi atau institusi dengan Pelaku Usaha sesuai peraturan perundang-undangan”.

Berikut beberapa kewenangan pemerintah dalam penyelenggaraan transaksi elektronik pada pasal 42 ayat 1 Peraturan Pemerintah 71/2019 mewajibkan bahwa penyelenggaraan transaksi elektronik harus menggunakan sertifikat elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik Indonesia. Pasal 43 mengharuskan penyelenggara sistem elektronik di sektor publik untuk memperhatikan aspek keamanan, keandalan, dan efisiensi. Pasal 45 ayat 2 Peraturan Pemerintah 71/2019 mengatur bahwa “Transaksi elektronik antara para pihak memiliki akibat hukum dan harus dilakukan dengan memperhatikan itikad baik, prinsip kehati-hatian, transparansi, akuntabilitas, dan kewajaran”.

Pada Pasal 50 PP 71/2019 menetapkan bahwa “Penyelenggaraan transaksi elektronik, para pihak harus memastikan penyampaian data dan informasi yang akurat, dan ketersediaan sarana serta layanan dan penyelesaian pengaduan”. PP 71/2019 Pasal 90 menjelaskan “Peran pemerintah dalam penyelenggaraan sistem dan transaksi elektronik, yang meliputi: memfasilitasi penggunaan teknologi informasi dan transaksi elektronik sesuai peraturan, melindungi kepentingan umum dari penyalahgunaan informasi elektronik dan transaksi elektronik yang dapat mengganggu ketertiban umum, mencegah penyebarluasan dan penggunaan informasi elektronik atau dokumen elektronik yang dilarang, menetapkan instansi atau institusi dengan data elektronik strategis yang perlu dilindungi”.

Pasal 91 menguraikan bahwa peran pemerintah dalam memfasilitasi penggunaan teknologi informasi dan transaksi elektronik sebagaimana pasal 90 termasuk: penetapan kebijakan, pelaksanaan kebijakan, fasilitasi infrastruktur, promosi dan edukasi, dan pengawasan”. Maka terdapat asas-asas dalam Kejahatan Teknologi Informasi Kejahatan teknologi informasi merupakan tindak pidana khusus yang diatur oleh Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11/2008 jo. UU No. 19/2016. Meskipun demikian, asas-asas umum dalam hukum pidana tetap relevan dan menjadi dasar pengaturan kejahatan ini dalam hukum nasional.

Beberapa asas-asas umum dalam hukum pidana yang relevan dengan kejahatan teknologi informasi meliputi:

1. Legalitas (*Nullum Crimen, Nulla Poena Sine Lege*), Prinsip ini menyatakan bahwa tidak ada kejahatan dan hukuman tanpa undang-undang yang mengaturnya terlebih dahulu.
2. Teritorialitas, Prinsip ini menyatakan bahwa hukum pidana berlaku dalam wilayah negara yang bersangkutan.
3. Nasional Aktif, Prinsip ini mengacu pada yurisdiksi negara atas kejahatan yang dilakukan oleh warganya, di mana pun kejahatan itu terjadi.
4. Nasional Pasif, Prinsip ini mengacu pada yurisdiksi negara atas kejahatan yang dilakukan terhadap warganya, meskipun kejahatan tersebut terjadi di luar wilayah negara.
5. Universal, Prinsip ini berlaku untuk kejahatan tertentu yang dianggap serius oleh masyarakat internasional, seperti terorisme atau kejahatan terhadap kemanusiaan, dan negara mana pun dapat menuntut pelaku kejahatan tersebut [20].

Meskipun asas-asas umum ini menjadi dasar pengaturan kejahatan teknologi informasi, pengecualian juga diatur dalam Pasal 2 UU ITE. Pasal ini menunjukkan bahwa kejahatan teknologi informasi juga melibatkan asas ekstrateritorial. Dengan demikian, pelaku yang melakukan kejahatan teknologi informasi di luar wilayah Indonesia tetap dapat dikenakan hukum berdasarkan UU ITE. Penegasan asas nasional pasif diperkuat dengan Pasal 37 UU ITE. Dalam menentukan *locus delicti* (tempat terjadinya kejahatan) dalam hukum pidana, ada tiga teori utama yang digunakan:

1. Teori Perbuatan Materiil mengacu pada tempat di mana tindakan kriminal dilakukan.
2. Teori Alat mengacu pada tempat di mana alat atau media yang digunakan dalam kejahatan berada.
3. Teori Akibat mengacu pada tempat di mana akibat dari kejahatan terjadi.

Namun, penerapan teori-teori ini dalam konteks kejahatan teknologi informasi menghadapi tantangan, mengingat proses kejahatan ini dapat melintasi batas negara melalui berbagai media dan menimbulkan akibat yang tidak terbatas pada satu negara saja.

Beberapa Teori Kedaulatan menjelaskan beberapa teori kedaulatan yang menjadi dasar pemikiran politik.

1. Teori Kedaulatan Tuhan menyatakan bahwa kedaulatan berasal dari Tuhan, di mana raja dianggap sebagai wakil Tuhan di bumi. Dalam pandangan ini, raja memiliki hak absolut untuk memerintah tanpa terikat oleh hukum atau kehendak rakyat. Teori ini berkembang pesat pada abad ke-16 dan ke-17 di Eropa, dengan contoh raja seperti Louis XIV dari Prancis yang mengklaim kedaulatan mutlak.
2. Teori Kedaulatan Rajaberpendapat bahwa raja memiliki kekuasaan penuh atas negaranya, tetapi sumber kekuasaan ini berasal dari kehendak rakyat, bukan dari Tuhan. Rakyat memberikan otoritas kepada raja melalui suatu kontrak sosial, sehingga raja dapat memerintah tanpa campur tangan pihak lain.
3. Teori Kedaulatan Hukum menekankan bahwa hukum merupakan sumber utama kedaulatan. Dalam teori ini, kedaulatan tidak terfokus pada individu, melainkan pada lembaga hukum dan konstitusi. Negara harus menghormati hukum dan kehendak rakyat, yang juga memiliki hak untuk mengubah konstitusi.
4. Teori Kedaulatan Rakyat menyatakan bahwa kedaulatan berasal dari rakyat, yang memiliki hak untuk menentukan bentuk pemerintahan dan kebijakan negara. Negara bertanggung jawab kepada rakyat dan harus mengakomodasi kepentingan mereka, menciptakan dasar bagi sistem demokrasi modern.
5. Teori Kedaulatan Kehendak Umum yang dikembangkan oleh Jean-Jacques Rousseau, menekankan bahwa kedaulatan terletak pada kehendak umum atau kepentingan bersama masyarakat. Negara harus mencerminkan dan mempromosikan kepentingan bersama tersebut [21].

Dari penjelasan ini, dapat disimpulkan bahwa Indonesia menganut teori kedaulatan rakyat, yang mengedepankan hak dan partisipasi masyarakat dalam pemerintahan.

Kejahatan teknologi informasi umumnya dibagi menjadi dua kategori utama:

1. Kejahatan yang menggunakan teknologi informasi sebagai media
2. Kejahatan yang menjadikan teknologi informasi sebagai sasaran

Delik dalam kejahatan teknologi informasi ini dapat dikelompokkan lebih lanjut sebagai berikut yaitu Delik terkait konten ilegal (Pasal 27-29 UU ITE), Delik terkait sistem elektronik (Pasal 30, 33 UU ITE), Delik terkait jaringan elektronik (Pasal 31 UU ITE), Delik terkait data/dokumen elektronik (Pasal 32, 35 UU ITE), Delik terkait fasilitasi kejahatan TI (Pasal 34 UU ITE), Delik tambaha (Pasal 36, 37 UU ITE).

Konvensi tentang Kejahatan Siber

Konvensi tentang Kejahatan Siber mengklasifikasikan berbagai jenis kejahatan siber menjadi beberapa kategori berikut:

1. Akses Ilegal meliputi tindakan mengakses sistem komputer atau data tanpa izin yang sah.
2. Intersepsi Ilegal mengacu pada penyadapan komunikasi data secara ilegal.
3. Gangguan Data berkaitan dengan pengubahan atau penghancuran data tanpa izin.
4. Gangguan Sistem termasuk tindakan yang mengganggu operasi normal sistem komputer.
5. Penyalahgunaan Perangkat meliputi penggunaan perangkat keras atau lunak untuk tujuan ilegal.
6. Pemalsuan Terkait Komputer berhubungan dengan pembuatan atau penggunaan dokumen palsu yang dibuat atau disimpan secara elektronik.
7. Penipuan Terkait Komputer termasuk tindakan penipuan yang dilakukan dengan menggunakan komputer atau sistem informasi.
8. Kejahatan Terkait Pornografi Anak menyangkut pembuatan, distribusi, dan kepemilikan materi pornografi anak.
9. Kejahatan Terkait Pelanggaran Hak Cipta dan hak-hak terkait yang dilakukan melalui media elektronik [22].

Masalah terbaru dalam yurisdiksi kriminal terhadap kejahatan siber muncul karena keunikan dan kompleksitas yang ditawarkan oleh lingkungan digital. Berbeda dengan kejahatan tradisional yang bersifat nyata dan terbatas pada ruang fisik tertentu, kejahatan siber sering kali melibatkan unsur "lintas batas abstrak," di mana tindakan kriminal dapat melintasi berbagai negara tanpa adanya batasan geografis yang jelas. Sebagai contoh, dalam kasus di mana mantan mahasiswa Jerman Barat berhasil mengakses sistem Departemen Pertahanan AS dengan menggunakan jaringan global yang melibatkan beberapa negara, ada pertanyaan mengenai apakah semua negara yang terlibat, termasuk Jepang, memiliki yurisdiksi atas kasus tersebut.

Perbedaan utama antara kejahatan siber dan kejahatan tradisional terletak pada fakta bahwa kejahatan siber dapat dilakukan tanpa adanya kontak langsung dengan subjek atau objek kejahatan, dan dampaknya sering kali jauh lebih luas. Pelaku kejahatan siber memanfaatkan perangkat seperti komputer dan ponsel untuk mengakses jaringan dan sistem di berbagai negara. Ini menimbulkan tantangan besar bagi teori tradisional mengenai yurisdiksi kriminal, di mana peraturan internasional dan perjanjian bilateral sering kali belum memadai untuk menangani kasus-kasus tersebut.

Sebagai contoh, jika seseorang mendirikan situs web pornografi di negara A, tetapi situs tersebut diakses oleh warga negara B, C, dan D, maka masing-masing negara mungkin merasa berhak untuk mengklaim yurisdiksi atas kasus tersebut. Negara B mungkin menganggap bahwa aktivitas warganya melanggar hukum pidana setempat, sementara negara C menganggap bahwa pendirian situs web pornografi itu sendiri adalah pelanggaran, dan negara D

mungkin merasa bahwa tindakan warganya melanggar norma hukum dan sosial lokal. Persaingan untuk yurisdiksi ini dapat mengakibatkan konflik, menyulitkan penyelesaian kasus, dan merugikan perlindungan hak serta kepentingan korban.

Prinsip-prinsip Pengamanan data, Pemerintah juga mengatur prinsip-prinsip pengamanan data pengguna dalam transaksi elektronik, yang mencakup kerahasiaan, integritas, dan keautentikan. Prinsip-prinsip ini penting untuk melindungi pengguna dalam ekosistem blockchain yang mungkin menghadapi berbagai risiko. Kewenangan dalam Melindungi Kepentingan umum maka pemerintah memiliki tanggung jawab untuk melindungi kepentingan publik dari potensi penyalahgunaan yang mungkin terjadi dalam transaksi elektronik. Ini termasuk penegakan hukum terhadap kejahatan teknologi informasi yang dapat muncul, termasuk penipuan atau pencurian data. Locus Delicti dalam kasus sengketa yang melibatkan transaksi teknologi informasi, pemerintah harus mempertimbangkan konsep locus delicti. Dengan sifat transaksi yang dapat melintasi batas negara, penting untuk menentukan di mana kejahatan terjadi dan yurisdiksi yang berlaku. Ini mencakup penerapan prinsip-prinsip baru dalam hukum yang terkait dengan kejahatan siber, seperti teori kedaulatan baru dan teori kontak minimal. Asas-asas Hukum Pidana, dalam menangani kejahatan yang terjadi di ruang siber, pemerintah harus mematuhi asas-asas hukum pidana, termasuk legalitas dan territorialitas, yang dapat menentukan tindakan hukum terhadap pelaku kejahatan.

Blockchain memiliki keunggulan utama berupa sifat desentralisasi, yang berkontribusi pada karakteristiknya yang tidak dapat diubah, aman, dan transparan. Namun, meskipun didukung oleh fitur-fitur ini, blockchain tetap rentan terhadap berbagai bentuk kejahatan. Kasus-kasus kejahatan yang terjadi di ekosistem blockchain dapat dibagi menjadi dua kategori utama yaitu kejahatan yang berasal dari smart contract dan pencurian aset kripto.

Kejahatan yang berkaitan dengan smart contract meliputi Rug Pull, Flash Loan Exploit, peretasan dompet kripto menggunakan metode Dusting dan Phishing, serta penipuan aset kripto melalui Fake Initial Coin Offering (ICO). Selain itu, kasus pencurian kepemilikan aset kripto juga sering terjadi, dengan berbagai modus peretasan, termasuk penggunaan rekayasa sosial. Metode rekayasa sosial adalah bentuk penipuan yang paling sering ditargetkan kepada para pemula di dunia kripto. Beberapa bentuk penipuan ini meliputi:

1. Helper Palsu dengan modus ini merupakan salah satu cara peretasan dompet kripto yang sering dijumpai, mengingat kebanyakan proyek kripto bersifat *self-service*.
2. Grup Telegram atau Sosial Media Palsu, banyak proyek blockchain yang memiliki grup di Telegram, Discord, atau Reddit, namun beberapa pihak memanfaatkan ini untuk membuat grup palsu yang tampak seolah-olah resmi.
3. Grup "Pump and Dump" dengan tujuan memanipulasi pasar dan meraup keuntungan. Banyak grup seperti ini dapat ditemukan di Telegram, yang menggunakan kata kunci "pump".
4. Giveaway Palsu dengan metode ini menargetkan pemula. Pelaku sering membuat video yang terlihat seolah-olah tokoh terkenal dalam dunia kripto, seperti Vitalik Buterin atau Elon Musk, sedang diwawancara [23].

Peristiwa hukum perdata terkait blockchain sering kali melibatkan masalah keabsahan dan perlindungan hak atas kontrak smart contracts dan transaksi di dalam ekosistem blockchain. Masalah utama dalam sengketa ini meliputi:

1. Smartcontract, yang dijalankan di atas blockchain, sering menghadapi tantangan hukum karena sifat anonim dan desentralisasi teknologi blockchain. Menurut Pasal 1330 KUH Perdata Indonesia, keabsahan kontrak memerlukan identitas jelas dari pihak-pihak yang terlibat. Namun, blockchain mempersulit identifikasi pihak karena anonimitas pengguna dan smart contract yang tidak mencantumkan identitas jelas. Ini mengakibatkan ketidakpastian mengenai keabsahan kontrak, karena sulit untuk memastikan bahwa semua syarat sahnya kontrak dipenuhi.
2. Sengketa sering timbul terkait dengan kepemilikan dan transfer aset kripto. Misalnya, jika aset kripto dicuri melalui peretasan atau penipuan, menentukan siapa yang berhak atas aset tersebut dan mendapatkan kembali aset yang hilang bisa menjadi rumit. Masalah ini diperparah jika aset tersebut dipindahkan atau dijual melalui transaksi yang tidak dapat dilacak dengan jelas.
3. Keterbatasan dalam penegakan hukum dapat menghambat pelaksanaan smart contract. Meskipun smart contract secara otomatis mengeksekusi ketentuan yang telah disepakati, penegakan hukum konvensional sering kali tidak bisa menjangkau tindakan yang melibatkan blockchain. Hal ini mengakibatkan kesulitan dalam mengadili pelanggaran kontrak atau penipuan yang melibatkan aset digital.
4. Berbagai negara memiliki regulasi yang berbeda mengenai blockchain dan aset kripto. Di Indonesia, ketidakpastian hukum mengenai penggunaan dan validitas smart contract, serta kurangnya regulasi khusus untuk bursa desentralisasi (DEX), menambah kompleksitas sengketa. Misalnya, platform seperti VexSwap dan DEJAVESwap yang belum terdaftar sebagai Penyelenggara Sistem Elektronik (PSE) menurut Kominfo, menghadapi tantangan hukum yang bisa mempengaruhi validitas dan perlindungan transaksi di platform tersebut.

Risiko Kriminal di Ekosistem Blockchain:

1. Pencurian aset bisa terjadi melalui pencurian kunci pribadi langsung atau teknik peretasan yang mencuri aset dari dompet atau bursa.
2. Penipuan bisa berupa penipuan untuk membeli aset palsu atau menawarkan imbal hasil yang tidak realistik untuk menarik dana penyedia likuiditas.
3. Pemalsuan transaksi bisa terjadi melalui manipulasi data transaksi di blockchain, seperti memalsukan jumlah atau alamat tujuan transaksi.

Secara umum, meskipun menjadi penyedia likuiditas bisa bermanfaat, penting untuk menyadari dan mengelola risiko-risiko ini dengan cermat untuk memastikan keselamatan dan keberhasilan investasi di ekosistem blockchain.

Pasal 40 UU ITE mengatur kewenangan pemerintah dalam hal ini:

1. Pemerintah memfasilitasi pemanfaatan teknologi informasi dan transaksi elektronik sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.
2. Pemerintah bertanggung jawab untuk melindungi kepentingan umum dari gangguan akibat penyalahgunaan informasi elektronik dan transaksi elektronik yang dapat mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan.

Pada Pasal 40 UU ITE, pemerintah memiliki kewenangan untuk bertanggung jawab untuk memfasilitasi pemanfaatan teknologi informasi dan transaksi elektronik sesuai dengan ketentuan peraturan perundang-undangan. Ini mencakup penerapan dan pengawasan terhadap standar teknis serta kebijakan yang mendukung penggunaan teknologi blockchain dan transaksi elektronik yang aman dan efisien. Pemerintah juga memiliki kewenangan untuk melindungi kepentingan umum dari gangguan akibat penyalahgunaan informasi elektronik dan transaksi elektronik. Ini termasuk menangani kasus-kasus yang mengganggu ketertiban umum, seperti penipuan digital, pelanggaran data, atau aktivitas ilegal yang dilakukan melalui teknologi blockchain.

Perlindungan ini bertujuan untuk menjaga integritas sistem transaksi elektronik dan memastikan bahwa hak-hak konsumen serta kepentingan publik terlindungi. Pemerintah juga memiliki kewenangan untuk mengeluarkan regulasi tambahan yang diperlukan untuk mengatasi perkembangan teknologi dan dinamika baru dalam transaksi elektronik. Ini termasuk pengaturan lebih lanjut mengenai keamanan siber, perlindungan data pribadi, dan mekanisme penyelesaian sengketa yang efektif. Secara keseluruhan, kewenangan hukum pemerintah Indonesia dalam menyelesaikan sengketa transaksi elektronik di ekosistem blockchain mencakup fasilitasi pemanfaatan teknologi, perlindungan kepentingan umum, dan penyediaan mekanisme penyelesaian sengketa yang komprehensif. Pemerintah berperan penting dalam memastikan bahwa sistem transaksi elektronik, termasuk blockchain, beroperasi secara adil, transparan, dan aman.

Ketika terjadi sengketa antara dua negara atau lebih terkait blockchain, kewenangan untuk menyelesaikan sengketa tersebut tergantung pada beberapa faktor penting. Berikut adalah penjelasan mengenai aspek-aspek yang perlu dipertimbangkan untuk menentukan kewenangan:

1. Penentuan Jurisdiksi
 - a. Lokasi dan Domisili Pihak, Jika salah satu pihak terletak di negara tertentu, negara tersebut dapat mengklaim yurisdiksi atas sengketa tersebut. Dalam banyak kasus, hukum nasional akan berlaku di mana pihak yang terlibat memiliki domisili atau lokasi fisik.
 - b. Klausul dalam Kontrak, Pihak-pihak dalam kontrak pintar dapat mencantumkan klausul yang menyatakan hukum mana yang akan berlaku dan di mana sengketa akan diselesaikan. Klausul ini biasanya mencakup pilihan untuk arbitrase atau pengadilan tertentu.
2. Metode Penyelesaian Sengketa
 - a. Penyelesaian Melalui Pengadilan Tradisional: Pengadilan tradisional dapat berusaha untuk menyelesaikan sengketa, tetapi seperti yang dijelaskan sebelumnya, ada banyak tantangan terkait interpretasi kode kontrak pintar dan verifikasi identitas pihak yang terlibat. Pengadilan mungkin juga mengalami kesulitan dalam menerapkan hukum yang relevan karena sifat desentralisasi dan anonim dari teknologi blockchain.
 - b. Arbitrase Internasional: Arbitrase sering dianggap lebih sesuai untuk sengketa yang melibatkan kontrak pintar. Arbitrase menyediakan fleksibilitas dalam memilih arbiter yang memiliki pemahaman mendalam tentang teknologi blockchain dan kontrak pintar. Dalam kasus ini, arbitrase bisa bersifat "off-chain" atau "on-chain", Off-chain menggunakan arbitrase tradisional di mana keputusan diambil secara konvensional, tetapi tetap didasarkan pada aturan yang dirancang khusus untuk teknologi blockchain. Sedangkan, On-chain, menggunakan platform yang mengintegrasikan keputusan arbitrase ke dalam smart contract, yang secara otomatis mengeksekusi putusan.
3. Pertimbangan Hukum Internasional
 - a. Perjanjian Bilateral atau Multilateral, Negara-negara yang terlibat mungkin memiliki perjanjian internasional yang mengatur penyelesaian sengketa. Ini dapat mencakup perjanjian perdagangan atau kerjasama teknologi yang menetapkan prosedur penyelesaian sengketa.

- b. Prinsip Ekstrateritorial dalam beberapa kasus, prinsip ekstrateritorial dapat diterapkan, di mana hukum negara dapat diterapkan terhadap tindakan yang dilakukan oleh warganya di luar negeri. Ini penting untuk memahami tanggung jawab di tingkat internasional.
4. Kendala yang Dihadapi, meskipun ada berbagai mekanisme untuk menyelesaikan sengketa, terdapat sejumlah tantangan yang harus dihadapi yaitu kesulitan dalam penegakan putusan, khususnya dalam konteks arbitrase on-chain, penegakan keputusan arbitrase dapat menjadi rumit. Potensi kelemahan keamanan dikarenakan platform arbitrase mungkin memiliki kerentanan yang dapat dieksplorasi. Rantai tanggung jawab yang rumit dalam konteks blockchain, sulit untuk menentukan siapa yang bertanggung jawab atas kesalahan, seperti kesalahan pengkodean [24].

Secara keseluruhan, untuk sengketa yang melibatkan teknologi blockchain antara dua negara, arbitrase internasional sering kali menjadi pilihan yang lebih menguntungkan dibandingkan dengan pengadilan tradisional. Kewenangan akan tergantung pada aspek-aspek seperti domisili pihak, hukum yang dipilih dalam kontrak, dan perjanjian internasional yang berlaku. Pihak-pihak yang terlibat harus mempersiapkan diri untuk beradaptasi dengan karakteristik unik dari teknologi blockchain dan potensi risiko yang menyertainya.

IV. SIMPULAN

Belum adanya regulasi khusus yang mengatur terkait dengan penerapan teknologi blockchain dalam transaksi elektronik secara komprehensif. Pemerintah Indonesia memiliki kewenangan hukum yang signifikan dalam menangani sengketa pada transaksi elektronik di ekosistem blockchain. Berdasarkan UU ITE No. 11 Tahun 2008, pemerintah bertanggung jawab untuk memastikan bahwa transaksi elektronik, termasuk yang berbasis blockchain, mematuhi prinsip kepastian hukum, kehati-hatian, dan itikad baik. Pasal 40 UU ITE menegaskan kewenangan pemerintah dalam memfasilitasi pemanfaatan teknologi informasi dan melindungi kepentingan umum dari penyalahgunaan informasi elektronik. Ini termasuk penegakan aturan untuk mencegah penipuan digital dan gangguan lainnya. Selain itu, pemerintah dapat mengeluarkan regulasi tambahan untuk mengatasi perkembangan teknologi dan penyelesaian sengketa, serta memastikan kepatuhan terhadap standar keamanan dan privasi. Dengan demikian, kewenangan pemerintah mencakup pengaturan, perlindungan, dan penyelesaian sengketa dalam transaksi blockchain, memastikan sistem yang adil dan aman untuk semua pihak.

UCAPAN TERIMA KASIH

Dengan tulus, penulis mengucapkan terima kasih kepada orang tua yang telah memberikan dukungan dan doa yang tiada henti, yang telah menjadi sumber kekuatan dan inspirasi selama proses penyelesaian artikel ini. Terima kasih juga kepada teman-teman yang telah memberikan bantuan, ide, dan motivasi yang berharga. Kepada semua pihak yang telah berkontribusi dalam penelitian ini, baik secara langsung maupun tidak langsung, penulis menyampaikan rasa terima kasih yang mendalam. Kontribusi semua pihak sangat penting dan membuat proses ini menjadi lebih lancar dan menyenangkan.

REFERENSI

- [1] E. I. Kadly, S. D. Rosadi, and E. Gultom, “Keabsahan Blockchain-Smart Contract Dalam Transaksi Elektronik: Indonesia, Amerika Dan Singapura,” *J. Sains Sosio Hum.*, vol. 5, no. 1, pp. 199–212, 2021, [Online]. Available: <https://www.academia.edu/download/76835346/11550.pdf>
- [2] V. Gupta, “A Brief History of Blockchain,” Harvard Business Review. Accessed: Jul. 21, 2024. [Online]. Available: <https://hbr.org/2017/02/a-brief-history-of-blockchain>
- [3] A. Anderberg *et al.*, *Blockchain Now And Tomorrow*. Luxembourg: Publications Office of the European Union, 2019. doi: doi:10.2760/901029.
- [4] Z. Ghozali *et al.*, *Manajemen Industri (Teori Komprehensif)*, Cetakan Pe. Yogyakarta: PT. Green Pustaka Indonesia, 2024. [Online]. Available: https://www.researchgate.net/publication/380461692_MANAJEMEN_INDUSTRI_Teori_Komprehensif/link/663d6aff06ea3d0b7446b8da/download?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwi cGFnZSI6InB1YmxpY2F0aW9uIn19
- [5] A. S. Subkhi and R. Rustam, “Perlindungan Hukum Investor atas Potensi Terjadinya Praktik Monkey Business dalam Transaksi Kripto di Bursa Komoditi,” *Pros. Semin. Huk. Aktual Fak. Huk. Univ. Islam Indones.*, vol. 2, no. 1, pp. 18–36, 2024, [Online]. Available: <https://jurnal.uii.ac.id/psha/article/view/33478>
- [6] S. M. N. Lase, A. Adinda, and R. D. Yuliantika, “Kerangka Hukum Teknologi Blockchain Berdasarkan Hukum Siber di Indonesia,” *Padjadjaran Law Rev.*, vol. 9, no. 1, pp. 1–20, 2021, [Online]. Available:

- <https://jurnal.fh.unpad.ac.id/index.php/plr/article/download/500/355>
- [7] D. C. Andrianto, "Perlindungan Hukum dan Pengenaan Pajak Bagi Investor Cryptocurrency di Indonesia," *J. Ilm. Univ. Batanghari Jambi*, vol. 22, no. 1, pp. 140–146, 2022, doi: <http://dx.doi.org/10.33087/jiubj.v22i1.2014>.
- [8] B. Raharjo, *Fintech: Teknologi Finansial Perbankan Digital*. Semarang: Yayasan Prima Agus Teknik Bekerja sama dengan Universitas Sains & Teknologi Komputer (Universitas STEKOM), 2021. [Online]. Available: <https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/144>
- [9] Z. Najafi, M. Taghadosi, K. Sharifi, and A. Farrokhanian, "The Effects of Inhalation Aromatherapy on Anxiety in Patients With Myocardial Infarction: A Randomized Clinical Trial," vol. 16, no. 8, 2014, doi: 10.5812/ircmj.15485.
- [10] A. Syamil *et al.*, *Buku Ajar Manajemen Rantai Pasok*, Cetakan Pe. Jambi: PT. Sonpedia Publishing Indonesia, 2023. [Online]. Available: https://www.researchgate.net/publication/373980212_Buku_Ajar_Manajemen_Rantai_Pasok/link/6506bcf39fdf0c69dfd20160/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn9
- [11] N. Chairunisah and G. Santoso, "Karakter Kebijaksanaan dalam Menghadapi Tantangan dan Peluang Abad ke-21 di Era Digital," *J. Pendidik. Transform.*, vol. 2, no. 5, pp. 452–475, 2023, doi: <https://doi.org/10.9000/jpt.v2i5.1612>.
- [12] M. T. Multazam, R. R. Phahlevi, M. I. Purnomo, S. B. Purwaningsih, and B. Sobirov, "Securing Blockchain Enterprises: Legal Due Diligence Amidst Rising Cyber Threats," *Padjadjaran J. Ilmu Huk.*, vol. 11, no. 1, pp. 26–52, 2024, doi: <https://doi.org/10.22304/pjih.v11n1.a2>.
- [13] M. T. Multazam, "Unleashing the Potential of DeFi: A Comprehensive Guide to Maximizing Rewards While Mitigating Risks," *Ganaya J. Ilmu Sos. Dan Hum.*, vol. 4, no. 3, pp. 906–918, 2021, doi: <https://doi.org/10.37329/ganaya.v4i3.2243>.
- [14] M. T. Multazam, R. A. Huzairin, S. P. Pratama, and Irwansyah, "Is It Legal to Provide Liquidity on the Vexanium Decentralized Exchange in Indonesia?," *Yust. J. Huk.*, vol. 12, no. 1, pp. 29–46, 2023, doi: <https://doi.org/10.20961/yustisia.v12i1.69007>.
- [15] R. M. Djati and T. I. D. W. P. Dewi, "Regulasi Metode Pembayaran Dengan Mata Uang Kripto (Cryptocurrency) Dalam Transaksi Bisnis Internasional," *Ethics Law J. Bus. Notary*, vol. 2, no. 2, pp. 91–106, 2024, doi: <https://doi.org/10.61292/eljbn.170>.
- [16] R. Tahir *et al.*, *Metodologi Penelitian Bidang Hukum (Suatu Pendekatan Teori dan Praktik)*, Cetakan Pe. Jambi: PT. Sonpedia Publishing Indonesia, 2023. [Online]. Available: https://www.researchgate.net/publication/375553399_METODOLOGI_PENELITIAN_BIDANG_HUKUM_Suatu_Pendekatan_Teori_dan_praktik/link/654ecb65b86a1d521bcc35df/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
- [17] Badan Pengawas Perdagangan Berjangka Komoditi, "Aset Kripto," Jakarta, 2020. [Online]. Available: https://bappebti.go.id/resources/docs/brosur_leaflet_2001_01_09_o26ulbsq.pdf
- [18] H. Hamid, *Hukum Perlindungan Konsumen Indonesia*, Cetakan I. Makassar: SAH Media, 2017.
- [19] Y. Fadhillah *et al.*, *Teknologi Blockchain dan Implementasinya*, Cetakan I. Bandung: Yayasan Kita Menulis, 2022.
- [20] M. T. Multazam, "Asas-asas dalam Kejahatan Teknologi Informasi," Wakelet. Accessed: Jul. 21, 2024. [Online]. Available: <https://wakelet.com/wake/-z0Tl4xzt64A4fAzn1mA1>
- [21] Tim Editor, "Pengertian Kedaulatan dan Teori-teorinya," Kumparan. Accessed: Nov. 03, 2024. [Online]. Available: <https://kumparan.com/pengertian-dan-istilah/pengertian-kedaulatan-dan-teori-teorinya-20fy08Z1Bcl>
- [22] X. Li and Y. Qin, "Research on Criminal Jurisdiction of Computer Cybercrime," *Procedia Comput. Sci.*, vol. 131, pp. 793–799, 2018, doi: <https://doi.org/10.1016/j.procs.2018.04.263>.
- [23] Y. Fadhillah, K. Samosir, R. A. Jamaludin, D. P. Y. Ardiana, A. M. A. K. Parewe, Y. S., J. Simarmata, A. F. Pakpahan, and M. T. Multazam, *Teknologi Blockchain dan Implementasinya*. Penerbit Yayasan Kita Menulis, pp. 97–106, 2022.
- [24] Z. Koray, "Blockchain, Smart Contracts and Alternative Dispute Resolution," Gide. Accessed: Nov. 03, 2024. [Online]. Available: <https://www.gide.com/en/news/blockchain-smart-contracts-and-alternative-dispute-resolution>

Conflict of Interest Statement:

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.