

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pada era saat ini, kemajuan teknologi digital telah mengalami perkembangan yang sangat pesat. Dengan berkembangnya teknologi tentu saja telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan manusia, sehingga penggunaannya dapat dimanfaatkan dalam berbagai hal. Namun demikian, di balik segala manfaat yang ditawarkan, teknologi digital juga membuka celah yang dapat dimanfaatkan oleh oknum tidak bertanggung jawab untuk melakukan berbagai bentuk kejahatan. Salah satu bentuk kejahatan yang paling mengkhawatirkan di era digital ini adalah kejahatan di dunia maya, yang dikenal dengan *cybercrime* atau kejahatan siber. Maraknya tindak kejahatan siber tersebut telah menimbulkan kekhawatiran yang serius di tengah masyarakat, karena tidak hanya mengancam keamanan data dan informasi pribadi, tetapi juga dapat merugikan secara finansial serta mengganggu ketertiban dan keamanan nasional.

Cybercrime merupakan suatu bentuk tindak pidana yang dilakukan dengan memanfaatkan teknologi komputer dan jaringan internet sebagai sarana utama untuk melaksanakan aksinya. Kejahatan tersebut tidak hanya membahayakan dan merugikan individu, tetapi juga suatu organisasi bahkan pemerintah juga tidak luput terkena dampak dari adanya kejahatan tersebut. Kejahatan siber memang tidak dapat dirasakan secara fisik namun sama merugikannya seperti pembunuhan, perampokan atau

pencurian¹. kejahatan siber tetap memiliki dampak yang sangat merugikan, baik secara materiil maupun immateriil, karena dapat menyebabkan kerugian finansial yang besar, pencurian data pribadi, gangguan terhadap sistem elektronik hingga ancaman terhadap keamanan nasional. Salah satu contoh *cybercrime* yang terjadi saat ini adalah "*Cryptojacking*". *Cryptojacking* yaitu tindakan dengan menyusupkan perangkat lunak ke dalam sistem komputer atau perangkat digital milik orang lain untuk memanfaatkan sumber daya perangkat tersebut. *Cryptojacking* merupakan metode terbaru dalam memecahkan algoritma guna mendapatkan mata uang digital tanpa sepengetahuan atau izin pemiliknya.

Cryptojacking memanfaatkan daya komputasi perangkat yang terinfeksi untuk menjalankan algoritma penambangan tanpa sepengetahuan pengguna². Kejahatan *cryptojacking* umumnya dilakukan dengan menyisipkan *malware* atau *torjan* ke dalam sistem, selain itu pelaku juga dapat menyematkan skrip pada situs web atau iklan digital dengan kode *javascript*. Dengan menyuntikkan kode penambangan ke situs web, sehingga pengguna tidak menyadari bahwa perangkat mereka sedang dimanfaatkan oleh pihak lain. Berbeda dengan jenis malware lainnya, tujuan utama *cryptojacking* bukanlah untuk merusak sistem pada komputer, akan tetapi memanfaatkan sumber

¹ Andreas Agung, Hafrida, Erwin, "Pencegahan Kejahatan Terhadap Cybercrime," *PAMPAS: Journal Of Criminal* 3 (2022): 212–22.

² Amanisa Rasyid Wiyani, "Cryptojacking; Malware Penambangan Kripto Secara Ilegal," Computer Security Incident Response Team UNAIR, accessed Maret 10, 2025, <https://csirt.unair.ac.id/cryptojacking-malware-penambangan-kripto-secara-ilegal/>

daya pemrosesan komputer korban guna mendapatkan mata uang kripto.³ Guna memperoleh mata uang kripto diperlukan biaya yang tinggi, diantaranya penggunaan daya komputasi yang besar, pembayaran tagihan listrik yang mahal, serta pembelian perangkat keras khusus. Maka dari itu, sebagian pelaku tidak ingin menanggung biaya tersebut sehingga memilih melakukan tindakan *cryptojacking*. *Cryptojacking* dapat dikategorikan berdasarkan cara terjadinya serangan, diantaranya sebagai berikut⁴ :

1. Peretasan kripto berbasis *host* : merupakan penyerangan yang membahayakan sistem *host* untuk memasang perangkat lunak peretasan kripto. Jenis ini terjadi ketika penyerang secara langsung menanamkan *malware* ke dalam komputer, laptop, atau *server* korban. *Malware* ini biasanya masuk lewat unduhan file mencurigakan, lampiran email, atau *software* bajakan.
2. *Cryptojacking* berbasis peramban : jika *cryptojacking* berasal dari kerentanan peramban atau berjalan sebagai subproses dari peramban Web yang disuplai, maka itu adalah *cryptojacking* berbasis peramban. Jenis ini lebih halus dan tidak perlu instalasi *malware*. Penyerang menyisipkan kode *Javascript* ke dalam sebuah website. Terdapat dua cara seseorang dapat menyusupkan kode JavaScript, yaitu dengan menyisipkan kode JavaScript ke website milik orang lain (misalnya melalui celah keamanan), dan yang kedua adalah ketika pemilik

³ Laith M Kadhum, Ahmad firdaus, Syifak I Hisham, Waheed Mushtaq, Moh Faial Ab Raak, “*Features, Analysis Techniques, an detection Methods of Cryptojacking Malware: A Survey*,” International journal On Informatics Visualization, no. 8 (Mei 2024): 891-896.

⁴ Sysdig, “Cryptomining vs Cryptojacking”, accessed Mei 19, 2025, <https://sysdig.com/learn-cloud-native/cryptomining-vs-cryptojacking/>

atau pengelola website itu sendiri turut menyisipkan kode JavaScript ke dalam websitenya. Ketika website tersebut diakses oleh pengguna lain, kode tersebut akan langsung berjalan secara otomatis sehingga korban tidak menyadari bahwa perangkatnya sedang dimanfaatkan.

3. *Cloud cryptojacking* : ketika *cryptojacking* terjadi pada infrastruktur *cloud*, seperti instans VM yang berjalan di *cloud* public, maka itu adalah serangan *cloud cryptojacking*. *Cloud* adalah layanan komputasi yang bisa digunakan lewat internet, tanpa perlu punya perangkat fisik sendiri seperti server atau data center. Ketika seseorang tidak punya komputer yang kuat, akan tetapi butuh menjalankan program berat. Dengan layanan *cloud*, kamu bisa “menyewa” komputer super kuat di internet untuk menjalankan programmu, lalu kamu tinggal mengaksesnya dari laptop biasa. Penyerang menyusup ke akun *cloud* seseorang atau organisasi, lalu menggunakan sumber daya *cloud* itu untuk menambang kripto dalam skala besar. Karena *cloud* punya daya komputasi tinggi, hasil tambangnya bisa besar, tetapi biaya server ditanggung korban.

Permasalahan *cryptojacking* tidak hanya menjadi ancaman bagi beberapa negara saja, Indonesia tidak luput dari serangan *cryptojacking*. Serangan *cryptojacking* pernah menargetkan salah satu portal berita ternama Indonesia yaitu ”Beritasatu.com“ pada bulan September 2017. Setelah diselidiki lewat prorses ”*Inspect Element-Sources*“, bahwasannya pelaku telah menyisipkan *script mining coin-have* yang berbasis koin monero pada laman portal tersebut. Permasalahan tersebut menyebabkan

kinerja CPU pembacanya langsung melonjak dan menetap di angka 100%. Setahun berselang munculnya serangan *cryptojacking* yang menargetkan pengguna router Mikrotik, 200.000 perangkat Mikrotik berhasil disusupi.

Berdasarkan laman Microsoft, microsoft telah merilis hasil penelitian Asia Pasifik di edisi terbaru “*Security Endpoint Threat Report 2019*” berdasarkan penelitian tersebut bahwasannya Indonesia menduduki peringkat tertinggi ke-4 di seluruh wilayah yaitu berada di 0,10 persen pada tahun 2019. Menurut laporan dari Perusahaan keamanan cyber Kaspersky, Indonesia mengalami peningkatan kasus *cryptojacking* sebesar 12% pada kuartal pertama tahun 2020, dengan lebih dari satu juta kasus penambangan ilegal terdeteksi di kalangan usaha kecil dan menengah. Tindak pidana pencucian uang dalam *cryptocurrency* juga meningkat, mencapai US\$8,6 miliar (sekitar Rp123,6 triliun) pada tahun 2021 ⁵.

Di zaman digital seperti saat ini mata uang digital atau yang sering dikenal dengan *cryptocurrency* menjadi salah satu media transaksi yang banyak diminati di berbagai kalangan masyarakat. Mata uang digital atau yang sering dikenal dengan *cryptocurrency* seperti *Bitcoin*, *Monero*, dan *Ethereum*. *Cryptocurrency* diamankan dengan suatu sistem yang disebut *kriptografi*. *Kriptografi* merupakan suatu teknik yang dalam penggunaannya memungkinkan untuk melakukan transaksi dengan

⁵ Irwan, Ary Julianto, “Orang Ini Hasilkan Kripto Senilai Rp 31,17 Miliar Hasil *Cryptojacking*” VOI, accessed 10 Maret 2025 https://voi.id/teknologi/348489/orang-ini-hasilkan-kripto-senilai-rp31-17-miliar-hasil-cryptojacking?utm_source=chatgpt.com

kerahasiaan informasi yang lebih aman dan memiliki tujuan untuk memberikan rasa nyaman berupa jaminan keamanan kepada penggunanya dengan tidak bisa diduplikasi maupun dijiplak. Prinsip dasar inilah yang kemudian menjadi fondasi dalam pengembangan teknologi *blockchain*. Dalam melakukan penambangan *cryptocurrency* tidak dapat dipisahkan dari keberadaan teknologi *blockchain*. Teknologi *blockchain* merupakan sistem penatatan transaksi yang digunakan untuk merekam setiap transaksi mata uang kripto secara aman, transparan, dan terdesentralisasi dan data transaksi tersebut menjadi permanen serta tidak dapat dirubah. Teknologi ini kemudian menjadi tulang punggung dalam aktivitas penambangan *cryptocurrency*, termasuk dalam proses validasi dan pembuatan mata uang digital. Pada dasarnya *cryptocurrency* merupakan mata uang yang tidak memiliki bentuk fisik akan tetapi berbentuk data informasi.⁶

Teknologi *blockchain* pada dasarnya bersifat netral dan digunakan untuk tujuan positif, yaitu untuk memastikan keamanan dan transparansi transaksi mata uang kripto. Akan tetapi, dalam konteks *cryptojacking*, teknologi *blockchain* menjadi wadah teknis yang secara tidak langsung dimanfaatkan dalam melakukan tindakan kejahatan. Teknologi *blockchain* memerlukan proses verifikasi transaksi yang disebut *minning*. Teknologi ini memiliki mekanisme *minning* yang membutuhkan daya komputasi sangat besar karena setiap transaksi harus diverifikasi dengan memecahkan puzzle kriptografi yang rumit. Proses inilah yang membuat *minning* hanya bisa dilakukan dengan

⁶ Farrel Sioe Christian, Tanaya Edgar Putu, “Regulasi Hukum Cryptocurrency Dan Pencegahan Tindak Penyalahgunaan Di Indonesia,” *Kertha Semaya: Journal Ilmu Hukum* 12, no. 6 (2024): 1375–86.

perangkat berperforma tinggi dan konsumsi energi yang besar proses tersebut yang menyerap banyak daya komputasi. Dengan demikian, teknologi blockchain bukanlah penyebab kejahatan, namun struktur dan mekanisme teknisnya yang mensyaratkan komputasi intensif secara tidak langsung menciptakan ruang bagi pelaku untuk mengambil keuntungan secara ilegal. *Cryptojacking* pada akhirnya merupakan bentuk penyalahgunaan proses *mining blockchain* dengan cara mengeksploitasi sumber daya perangkat milik orang lain, sehingga menimbulkan kerugian baik dari segi kinerja perangkat maupun konsumsi energi.

Fenomena *cryptojacking* yang memanfaatkan teknologi blockchain secara tidak sah menunjukkan bahwa kemajuan teknologi. Kemajuan teknologi tidak hanya membawa manfaat, tetapi juga membuka peluang bagi munculnya bentuk-bentuk kejahatan baru yang kompleks dan sulit dideteksi, di mana teknologi ini justru menjadi celah bagi pelaku kejahatan siber untuk memperoleh keuntungan pribadi. Kejahatan ini tidak hanya menimbulkan kerugian secara ekonomi dan teknis, tetapi juga menghadirkan tantangan dalam aspek pertanggungjawaban pidana. Karakteristik kejahatan siber seperti *cryptojacking* yang tidak merusak secara fisik namun mengeksploitasi sumber daya sistem membuktikan bahwa instrumen hukum konvensional seperti Kitab Undang-undang Hukum Pidana (yang selanjutnya disebut dengan KUHP) memiliki keterbatasan dalam menjangkau bentuk-bentuk kejahatan modern yang berbasis teknologi informasi, yang dilakukan tanpa interaksi fisik

langsung serta melibatkan teknologi yang berkembang secara dinamis tidak selalu memiliki jejak digital yang jelas.

Keterbatasan KUHP dalam menjangkau dan mengantisipasi berbagai bentuk kejahatan modern, inilah yang mendorong lahirnya berbagai instrument hukum pidana di luar KUHP, salah satunya adalah Undang-Undang No.1 Tahun 2024 tentang perubahan kedua atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut dengan UU ITE). Hal ini sejalan dengan Undang-undang Informasi dan Transaksi Elektronik (UU ITE) yang secara khusus mengatur perbuatan melawan hukum yang dilakukan melalui sistem elektronik dan teknologi informasi. UU ITE dirancang untuk mengisi kekosongan hukum dalam menghadapi kejahatan di dunia maya yang tidak terakomodasi secara memadai dalam KUHP. Dalam konteks ini, UU ITE tidak hanya memberikan landasan hukum terhadap transaksi elektronik dan perlindungan data, tetapi juga memberikan sanksi pidana terhadap berbagai bentuk serangan siber.

Meskipun kerangka hukum seperti Undang-undang Informasi dan Transaksi Elektronik telah berupaya mengatur berbagai bentuk kejahatan siber, perkembangan teknologi digital yang begitu pesat menimbulkan tantangan baru dalam penerapannya. Namun demikian, dikarenakan *cryptojacking* berkaitan langsung dengan teknologi *blockchain* dan mekanisme penambangan *cryptocurrency* yang masih tergolong baru di Indonesia, muncul tantangan dalam menafsirkan unsur-unsur tindak pidana dalam

UU ITE, terutama mengenai batasan melawan hukum, serta bentuk pertanggungjawaban pelaku.

Walaupun tindak kejahatan *cryptojacking* tidak menyebabkan kerusakan pada komputer, akan tetapi *cryptojacking* perlu menjadi perhatian yang serius di kalangan penegak hukum dan Masyarakat, mengingat dampaknya yang merugikan baik secara ekonomi maupun sosial. Selain itu *Cryptojacking* juga berpotensi digunakan untuk mendukung aktivitas ilegal lainnya, seperti pencucian uang atau pendanaan kejahatan terorganisir. Di Indonesia, meskipun telah ada beberapa regulasi yang mengatur tentang kejahatan siber, seperti Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi elektronik (UU ITE). Dalam konteks pengaturan tindak pidana yang berkaitan dengan pemanfaatan sistem elektronik secara tidak sah, salah satu ketentuan yang memiliki relevansi penting untuk dikaji lebih lanjut adalah ketentuan mengenai akses ilegal terhadap sistem elektronik yang dimana termuat dalam Pasal 30 Undang-undang No 11 Tahun 2008. Berdasarkan Pasal 30 Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menyatakan bahwa

- 1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
- 2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau sistem elektronik engan ara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.
- 3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Berkaitan dengan pengaturan akses ilegal dalam sistem elektronik, Pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi salah satu ketentuan yang relevan untuk dianalisis. Ketentuan ini telah mengalami dua kali perubahan, yaitu melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024. Pada perubahan pertama melalui UU ITE Nomor 19 Tahun 2016, perubahan hanya berupa penyisipan angka 6a dalam Pasal 1 serta perubahan terhadap Pasal 26, Pasal 31, Pasal 40, Pasal 43, Pasal 45, Pasal 45A, dan Pasal 45B. Selanjutnya, perubahan kedua melalui UU ITE Nomor 1 Tahun 2024 mencakup perubahan terhadap Pasal 13, Pasal 13A, Pasal 16A, Pasal 16B, Pasal 17, Pasal 18A, Pasal 27, Pasal 27A, Pasal 27B, Pasal 28, Pasal 29, Pasal 36, Pasal 40, Pasal 40A, Pasal 43, Pasal 45, Pasal 45A, dan Pasal 45B. Berdasarkan kedua perubahan tersebut, dapat disimpulkan bahwa Pasal 30 UU ITE tidak mengalami perubahan, sehingga rumusan norma mengenai akses tanpa hak terhadap sistem elektronik tetap berlaku sebagaimana ketentuan awalnya.

Dalam Undang-Undang N0. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada pasal 30 dijelaskan mengenai modus operandi dari hacking yang biasanya disebut “*Unauthorized Access to Computer System and Service*” yang memiliki arti tindakan kejahatan yang secara ilegal dilakukan dengan mengakses atau menembus ke dalam jaringan komputer tanpa sepengetahuan dari pemilik sistem, biasanya pelaku melakukan modus sebagaimana dimaksud guna men-sabotase

atau mencuri data dan informasi rahasia⁷. Berbeda halnya dengan *cryptojacking*, Meskipun Pasal 30 UU ITE secara tegas melarang setiap orang melakukan akses tanpa hak terhadap sistem elektronik, rumusan pasal tersebut secara substansial hanya menitikberatkan pada aspek intrusi atau penerobosan sistem. Norma ini belum menjangkau secara spesifik tindakan pemanfaatan sumber daya komputasi milik orang lain setelah akses tersebut terjadi. Dalam praktik *cryptojacking*, pelaku tidak melakukan pencurian data, pengubahan informasi, atau perusakan sistem, tetapi justru mengeksploitasi kapasitas *CPU*, *memori*, *bandwidth*, serta energi listrik perangkat korban untuk melakukan penambangan *cryptocurrency*. Aktivitas tersebut secara nyata menimbulkan kerugian, namun tidak ditemukan pengaturan tegas dalam UU ITE yang mengkualifikasikan penggunaan sumber daya komputasi tanpa izin sebagai perbuatan terlarang.

Meskipun Pasal 30 UU ITE secara tegas melarang setiap orang melakukan akses tanpa hak terhadap sistem elektronik, rumusan pasal tersebut secara substansial hanya menitikberatkan pada aspek intrusi atau penerobosan sistem. Norma ini belum menjangkau secara spesifik tindakan pemanfaatan sumber daya komputasi milik orang lain setelah akses tersebut terjadi. Ruang lingkup Pasal 30 UU ITE saat ini masih terbatas dan tidak mencakup perbuatan *cryptojacking* yang dilakukan melalui penyisipan kode *JavaScript* pada website atau aplikasi milik pelaku sendiri untuk

⁷ Bramanta Aryo Wijoseno, I Gusti A A D Widhiyaastuti, “Jerat Pidana Terhadap Pelaku Peretas Sistem Komputer Secara Ilegal (Hacker) Dalam Perspektif Hukum Pidana Indonesia,” Jurnal Kertha Desa, Vol. 11, No. 3 (2023): 2031-2041.

mengeksploitasi sumber daya komputasi pengguna. Kekaburan pengaturan inilah yang menciptakan ketidakjelasan mengenai batasan delik dan kepastian dalam menentukan pertanggungjawaban pidana bagi pelaku *cryptojacking*. Padahal dampak yang ditimbulkan juga merugikan korban, mengingat pelaku *cryptojacking* sering kali tidak mencuri data atau merusak sistem, melainkan hanya menjalankan operasi pengambilan mata uang kripto yang terkadang tidak disadari oleh korban. Kekaburan dan keterbatasan norma menyebabkan ketidakjelasan dalam menentukan unsur sifat melawan hukum serta dasar pertanggungjawaban pidana bagi pelakunya. Kondisi ini menunjukkan adanya kesenjangan antara perkembangan kejahatan berbasis teknologi dengan konstruksi norma dalam Pasal 30 UU ITE.

Perkembangan teknologi yang terus berubah menuntut adanya adaptasi dalam sistem hukum yang ada. Seiring meningkatnya penggunaan mata uang digital *cryptocurrency* dan tingginya risiko *cryptojacking* sebagai bentuk kejahatan siber, diperlukannya perhatian yang lebih guna memberantas kejahatan tersebut. Oleh karena itu, penelitian ini penting untuk menafsirkan ketentuan Pasal 30 UU ITE agar dapat menentukan pertanggungjawaban pidana pelaku *cryptojacking*. Sejalan dengan itu, penelitian ini diarahkan untuk memastikan bagaimana pelaku *cryptojacking* dapat dimintai pertanggungjawaban pidana dan untuk mengevaluasi sejauh mana UU ITE telah memberikan pengaturan yang jelas terkait tindak pidana tersebut. Berdasarkan penjelasan tersebut patut untuk dilakukan penelitian mengenai Pertanggungjawaban Pelaku *Cryptojacking* Sebagai *Cybercrime* Dalam Hukum Pidana Indonesia.

1.2 Rumusan Masalah

Maka dari itu dengan adanya permasalahan tersebut penelitian ini merumuskan :

1. Apakah *Cryptojacking* merupakan suatu tindak pidana di Indonesia?
2. Apakah konsep pertanggungjawaban dalam Undang-undang No 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dapat diterapkan terhadap pelaku tindak pidana *cryptojacking*?

1.3 Tujuan Penelitian

Berdasarkan permasalahan yang telah dipaparkan sebelumnya, maka tujuan dari penelitian ini adalah untuk :

1. Untuk menganalisa apakah *Cryptojacking* merupakan suatu tindak pidana di Indonesia
2. Untuk menganalisa apakah konsep pertanggungjawaban dalam Undang-undang No 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dapat diterapkan terhadap pelaku tindak pidana *cryptojacking*

1.4 Kegunaan Penelitian

a) Kegunaan Teoritis

Hasil dari penelitian ini diharapkan dapat menambah wawasan, pengetahuan, dan pemahaman bagi pembaca maupun peneliti sendiri. Selain itu dengan adanya penelitian ini diharapkan dapat memberikan kontribusi dalam

pengembangan ilmu hukum pidana. Sehingga dapat dijadikan tambahan bahan informasi oleh peneliti selanjutnya.

b) Kegunaan Praktis

Dengan adanya penelitian ini diharapkan hasil yang diperoleh dapat dijadikan sebagai bahan acuan dan pertimbangan bagi para penegak hukum dalam menghadapi dan menentukan permasalahan yang sesuai dengan topik penelitian.

1.5 Keaslian Penelitian

Penelitian yang penulis laksanakan dengan mengangkat judul “PERTANGGUNGJAWABAN PELAKU CRYPTOJACKING SEBAGAI CYBERCRIME DALAM HUKUM PIDANA INDONESIA” merupakan topik yang sebelumnya telah diteliti dalam sejumlah skripsi dan karya ilmiah lainnya, meskipun dengan judul yang berbeda.

No .	Judul Penelitian Sebelumnya	Rumusan Masalah Penelitian Sebelumnya	Isu Hukum Penelitian Sebelumnya	Perbedaan Dengan Tugas Akhir Yang Diusulkan
1.	Irham Nurroziqi Universitas Wijaya Kusuma Surabaya Fakultas Hukum Program Studi Hukum Program	Siapa sajakah pelaku tindak pidana yang terdapat di dalam kejahatan siber (Cybercrime) dalam mata uang kripto (Cryptocurrency)	Menganalisis bentuk-bentuk kejahatan siber dalam cryptocurrency dan bagaimana pertanggungjawaban pidana bagi pelakunya	Perbedaannya yakni Menganalisis bentuk-bentuk kejahatan siber dalam cryptocurrency dan bagaimana pertanggungjawaban pidana bagi pelakunya.

	Sarjana Karya Ilmiah Thesis 2022 ”Pertanggungjawaban Pidana Terhadap Pelaku Kejahatan Cyber (Cybercrime) Dalam Mata Uang Kripto (Cryptocurrency)”	Bagaimanakah pertanggungjawaban pidana bagi pelaku tindak pidana kejahatan siber (Cybercrime) dalam mata uang kripto (Cryptocurrency)		Sedangkan pada peneliti yang akan dilakukan hanya berfokus kepada cryptojacking, sedangkan pada karya ilmiah tersebut masih belum dibahas kejahatan siber cryptojacking. Dimana cryptojacking berfokus pada penyalahgunaan sumber daya computer korban untuk menambang mata uang kripto tanpa izin
2.	Irfan Murtadha Program Studi Hukum Pidana Islam Fakultas Syariah Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember Skripsi Juni 2024 “Tindak Pidana Pencucian Uang Menggunakan Cryptocurrenc	Bagaimana pembuktian dari tindak pidana pencucian uang menggunakan Cryptocurrency atau asset kripto ? Bagaimana ketentuan pidana mengenai tindak pidana pencucian uang menggunakan Cryptocurrency atau asset kripto dalam hukum positif di Indonesia?	Membahas mengenai cara pembuktian seseorang yang melakukan TPPU dengan menggunakan Cryptocurrency serta bagaimana ketentuan pidana seseorang yang melakukan TPPU dengan menggunakan cryptocurrency	Perbedaannya yakni pada penelitian sebelumnya membahas mengenai cara pembuktian seseorang yang melakukan TPPU dengan menggunakan Cryptocurrency serta bagaimana ketentuan pidana seseorang yang melakukan TPPU dengan menggunakan cryptocurrency sedangkan pada

	y Di Indonesia”			penelitian yang akan dilakukan yaitu mengenai pertanggungjawaban cryptojacking dimana pelaku tindak pidana tersebut mencari keuntungan secara finansial dengan melakukan penambangan mata uang digital crypto secara ilegal
3.	Syabilah Yuka Kawandoda Fakultas Hukum Universitas Muslim Indonesia Makassar 2022 Skripsi “Penanggulang an Kejahatan Cyber Crime Yang Dilakukan Oleh Hacker Dalam Tinjauan Kejahatan Internasional (Studi Kasus Cyber Polda Sulsel)”	Bagaimanakah bentuk kejahatan cyber yang dilakukan oleh hacker dalam tinjauan hukum kejahatan Internasional? Bagaimanakah efek yang ditimbulkan oleh serangan Hacker dan implikasinya terhadap pertahanan dan keamanan Negara ?	Membahas menegani kejahatan cyber yang berupa phising dalam sudut pandang internasional beserta dampak yang ditimbulkan terhadap pertahanan dan keamanan Negara beserta upaya yang dilakukan oleh Polda Sulsel dalam menangani tindak kejahatan cyber yang dilakukan oleh hacker	Perbedaannya yakni pada penelitian sebelumnya membahas menegani kejahatan cyber yang berupa phising. dalam sudut pandang internasional beserta dampak yang ditimbulkan terhadap pertahanan dan keamanan Negara beserta upaya yang dilakukan oleh Polda Sulsel dalam menangani tindak kejahatan cyber yang

				dilakukan oleh hacker. Dimana, phising sendiri dapat diartikan sebagai penggunaan situs web atau email palsu (seolah-olah asli) untuk mencuri data, yang merupakan bentuk manipulasi informasi elektronik agar dianggap otentik. Sedangkan cryptojacking dapat diartikan sebagai sedangkan pada penelitian yang akan dilakukan objeknya yaitu mengenai pertanggungjawaban pelaku cryptojacking dimana pelaku tindak pidana tersebut mencari keuntungan secara finansial dengan melakukan penambangan mata uang digital crypto secara illegal
--	--	--	--	---

Ketika menyusun penelitian skripsi tentang Pertanggungjawaban Pelaku *Cryptojacking* Sebagai *Cybercrime* Dalam Hukum Pidana Indonesia, telah dilakukan perbandingan dengan beberapa penelitian skripsi yang telah ada sebelumnya. sehingga dengan dilakukannya perbandingan dapat ditemukan adanya perbedaan antara penelitian skripsi sebelumnya dengan penelitian skripsi yang akan dilakukan. Adapun dalam penelitian pertama dan kedua sama-sama mengkaji mengenai *cryptocurrency*. *Cryptocurrency* merupakan sebuah bentuk mata uang digital atau mata uang virtual yang menggunakan *kriptografi* guna menjamin keamanan dalam setiap transaksi. Berbeda dengan mata uang tradisional seperti rupiah yang dikeluarkan oleh pemerintah. *Cryptocurrency* tidak terpusat dan umumnya berjalan di atas teknologi *blockchain*, yaitu sistem pencatatan digital yang tersebar di berbagai komputer di seluruh dunia. Contoh mata uang digital yang paling terkenal adalah *bitcoin*. *Crptocurrency* sering dimanfaatkan dalam berbagai bentuk kejahatan karena sifatnya yang anonym dan sulit dilacak, salah satu bentuk kejahatan tersebut ialah tindak pidana pencucian uang dimana telah diteliti oleh peneliti ke dua.

Terkait hal tersebut terdapat perbedaan antara kejahatan *cryptojacking* dengan bentuk kejahatan lainnya, meskipun keduanya sama-sama bertujuan untuk memperoleh mata uang kripto. *Cryptojacking* merupakan suatu tindak kejahatan siber dimana seseorang secara diam-diam memanfaatkan sumber daya perangkat komputer atau gadget milik orang lain untuk menambang *cryptocurrency* tanpa izin pemilik perangkat tersebut. *Crptojacking* berbeda dengan kejahatan lainnya karena pelakunya

memanfaatkan perangkat korban secara tersembunyi tanpa melakukan pencurian langsung atau transaksi ilegal, sehingga sifatnya lebih tersembunyi akan tetapi tetap merugikan.

1.6 Metode Penelitian

Penelitian merupakan suatu kegiatan ilmiah yang berkaitan dengan analisa dan konstruksi, yang dilakukan secara metodologis, sistematis dan konsisten. Penelitian hukum merupakan suatu kegiatan ilmiah yang didasarkan pada metode, sistematika, dan pemikiran tertentu, yang bertujuan untuk mempelajari satu atau beberapa gejala hukum tertentu dengan jalan menganalisisnya, kecuali itu, juga diadakan pemeriksaan yang mendalam terhadap fakta hukum tersebut untuk kemudian mengusahakan suatu pemecahan atas permasalahan-permasalahan yang timbul di dalam gejala yang bersangkutan.⁸

1.6.1 Jenis Penelitian

Adapun jenis penelitian yang digunakan dalam penelitian ini adalah jenis penelitian hukum normatif. E. Saefullah Wiradipradja menguraikan bahwa, penelitian hukum normatif merupakan “penelitian hukum yang mengkaji norma hukum positif sebagai obyek kajiannya”⁹. Penelitian hukum normatif (*legal research*) biasanya “hanya” merupakan studi dokumen, yakni menggunakan sumber bahan hukum yang berupa peraturan perundang-

⁸ Zainuddin Ali, *Metode Penelitian Hukum* (Sinar Grafika, 2021), 14.

⁹ Muhaimin, *Metode Penelitian Hukum*(Mataram-NTB: UPT. Mataram Univerity Pers, 2020)

undangan, keputusan/ketetapan pengadilan, kontrak/perjanjian/akad, teori hukum, dan pendapat para sarjana.¹⁰ Sebagaimana juga yang dipaparkan oleh Peter Mahmud Marzuki yang menyatakan bahwa “..... Penelitian Hukum Normatif dilakukan untuk menghasilkan argumentasi, teori atau konsep baru sebagai prenskripsi dalam menyelesaikan masalah yang dihadapi.....”¹¹ Penelitian ini mempunyai tujuan guna memberikan argumentasi hukum yang digunakan sebagai dasar penentu apakah suatu peristiwa telah benar atau salah serta bagaimana sebaiknya peristiwa itu menurut hukum.¹²

1.6.2 Pendekatan Penelitian

Sebagai bagian dari penelitian di bidang hukum, isu hukum yang menjadi fokus kajian akan menentukan jenis pendekatan yang digunakan, sehingga pendekatan tersebut harus disesuaikan dengan permasalahan yang akan dianalisis dalam penelitian. Adapun pendekatan yang digunakan dalam penelitian ini yaitu :

1. Pendekatan perundang-undangan (*statue approach*)

Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi yang terkait dengan isu hukum yang sedang bahas (diteliti)¹³. Penelitian ini mengkaji berbagai

¹⁰ *Ibid*, 45

¹¹ Peter Mahmud, "*Penelitian Hukum (Edisi Revisi)*" (Jakarta: PT. Kencana, 2021). Hlm 42

¹² Mukti Fajar and Yulianto Achmad, "*Dualisme Penelitian Hukum Normatif Dan Empiris, Cetakan IV,*" Yogyakarta: Pustaka Pelajar 280 (2017): 36.

¹³ Muhaimin, "*Metode Penelitian Hukum*" (Mataram-NTB: UPT. Mataram Universitas)

ketentuan hukum yang tercantum dalam sejumlah peraturan perundang-perundang, diantaranya :

- a. Undang-undang No. 11 tahun 2008 tentang Informasi dan Elektronik
- b. KUHP Lama
- c. Undang-undang No 1 Tahun 2023 (KUHP Baru)
- d. Undang-undang No. 27 tahun 2022 tentang perlindungan data pribadi

2. Pendekatan konseptual (*conceptual approach*)

Di samping menerapkan pendekatan perundang-undangan, penelitian ini juga menggunakan pendekatan konseptual (*conceptual approach*). Peneliti perlu merujuk kepada prinsip-prinsip hukum. Prinsip-prinsip ini dapat diketemukan dalam pandangan-pandangan sarjana ataupun doktrin-doktrin hukum¹⁴. Pendekatan konseptual dalam membahas pertanggungjawaban pelaku *cryptojacking* sebagai *cybercrime* menitikberatkan pada pemahaman teori-teori hukum pidana, konsep *cybercrime*, serta prinsip legalitas dalam sistem hukum Indonesia. Dalam penelitian ini, pendekatan tersebut digunakan untuk memahami dan mengkaji konsep pertanggungjawaban pidana pelaku *cryptojacking*, yang

¹⁴ Peter Mahmud, “*Penelitian Hukum (Edisi Revisi)*” (Jakarta PT: kencana, 2017). Hlm 178

merupakan salah satu bentuk tindak pidana siber, berdasarkan asas dan doktrin hukum pidana Indonesia yang relevan. Hal ini mencakup kajian terhadap pandangan serta doktrin para ahli hukum pidana terkait unsur kesalahan dan bentuk pertanggungjawaban pidana, terutama dalam konteks kejahatan siber. Penelaahan ini juga menjadi penting mengingat belum adanya aturan yang secara spesifik mengatur tentang teknologi *blockchain* dalam sistem hukum nasional. Pendekatan ini digunakan untuk memberikan penguatan dalam menganalisis isu hukum melalui pemahaman teoritis dan konseptual, sehingga hasil penelitian memiliki dasar yang kuat.

1.6.3 Sumber Bahan Hukum

Dalam penelitian hukum normatif, sumber bahan hukum merupakan suatu elemen yang penting untuk digunakan sebagai dasar analisis terhadap permasalahan hukum yang dikaji. Sumber-sumber penelitian hukum dapat dibedakan menjadi sumber-sumber penelitian yang berupa bahan-bahan hukum primer dan bahan-bahan hukum sekunder.¹⁵ Pada tahap pengumpulan data adapun bahan hukum yang digunakan :

1. Bahan Hukum Primer

Bahan hukum primer merupakan sumber hukum utama. Bahan hukum primer merupakan bahan hukum yang bersifat autoritatif, artinya mempunyai

¹⁵ Peter Mahmud, *Penelitian Hukum (Edisi Revisi)* (Jakarta: PT. Kencana, 2021). Hlm 181

otoritas.¹⁶ Bahan ini menjadi dasar utama dalam menganalisis permasalahan hukum karena memuat aturan-aturan hukum yang berlaku secara formal. Adapun bahan hukum yang digunakan :

- a. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- b. Undang-undang No. 1 Tahun 2023 (Kitab Undang-Undang Hukum Pidana Baru)
- c. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi
- d. Kitab Undang-Undang Hukum Pidana (Lama)

2. Bahan Hukum Sekunder

Bahan hukum sekunder merupakan bahan hukum yang memberikan penjelasan atau analisis terhadap bahan hukum primer. Dalam penelitian ini bahan hukum sekunder digunakan untuk memperkuat analisis bahan hukum primer dengan merujuk pada sumber Hukum yang diperoleh dari buku, jurnal Hukum, artikel Hukum, serta sumber lainnya yang berkaitan dengan isu Hukum yang dikaji dalam penelitian ini

1.6.4 Teknik Pengumpulan Bahan Hukum

Teknik pengumpulan bahan hukum yang digunakan penelitian ini adalah teknik pengumpulan bahan hukum melalui studi kepustakaan. Studi pustaka (*bibliography study*); adalah pengkajian informasi tertulis mengenai

¹⁶ Ibid

hukum yang berasal dari berbagai sumber dan dipublikasikan secara luas serta dibutuhkan dalam penelitian hukum normatif.

1.6.5 Analisis Bahan Hukum

Analisis bahan hukum disebut sebagai kegiatan yang memberikan telaah, yang dapat berarti menentang, mengkritik, mendukung, menambah, dan memberi komentar serta kemudian membuat suatu kesimpulan terhadap hasil penelitian berdasarkan pikiran sendiri dengan bantuan teori.¹⁷ Pada penelitian ini, setelah seluruh bahan hukum yang relevan berhasil dikumpulkan, tahap selanjutnya adalah menganalisis bahan-bahan tersebut. metode analisis yang diterapkan dalam penelitian ini bersifat kualitatif, yaitu dengan melakukan penafsiran terhadap bahan hukum yang telah diolah, guna memperoleh pemahaman yang mendalam terhadap isu hukum yang diteliti.

¹⁷ Mukti Fajar and Yulianto Achmad, *Dualisme Penelitian Hukum Normatif Dan Empiris* (Yogyakarta: Pustaka Pelajar, 2010).