PERADABAN JOURNAL OF LAW AND SOCIETY

Article

Should Crypto Mining Without Consent Be Criminalized? Lessons from the Coinhive Decision

Lucky Elza Aditya[1], Silvy Chintia Adelia[2], Firly Amalia Rafi Ridha

[1] Universitas Brawijaya, Malang, Indonesia;
email : luckyelza@ub.ac.id

[2] Universitas Negeri Surabaya, Surabaya, Indonesia;
email : silvyadelia@unesa.ac.id

[3] Universitas Negeri Surabaya, Surabaya, Indonesia;
email : firlyarr@student.ub.ac.id

Abstract

This article examines whether crypto mining conducted without user consent should be criminalized under Indonesian cybercriminal law by drawing lessons from the Japanese Supreme Court's Coinhive Decision. The study employs normative legal research using statutory, case, and comparative approaches to analyze Indonesian cybercrime legislation and the legal reasoning adopted in the Coinhive Decision. Unlike previous studies that primarily discuss cryptojacking from technical or criminal liability perspectives, this research develops a comparative framework that positions informed user consent and the degree of interference with electronic systems as the principal parameters for determining criminal liability. The findings demonstrate that cryptojacking should be criminalized only when it is conducted without valid user consent and results in significant interference with electronic systems, unauthorized exploitation of computing resources, or other measurable harm to users. Conversely, transparent cryptomining conducted pursuant to valid digital agreements should not automatically be regarded as a criminal offense because the elements of unlawfulness and unauthorized conduct are absent. This study contributes to Indonesian cybercriminal law by proposing clearer normative parameters for distinguishing lawful cryptomining from criminal cryptojacking, drawing on the principles of user consent, proportionality, and social acceptance reflected in the Coinhive Decision.

Keywords

Cryptojacking, Criminal Liability, Finance Crime, Digital Consent, Cyber Criminal Law

PERADABAN JOURNAL OF LAW AND SOCIETY
Vol. 5, Issue 1, June 2026

E-ISSN: 2830-1757

Page : 95-110

DOI : https://doi.org/10.59001/pjls.v5i1.861

Abstrak

Artikel ini mengkaji apakah aktivitas penambangan mata uang kripto tanpa persetujuan pengguna patut dikriminalisasi dalam hukum pidana siber Indonesia dengan mengambil pelajaran dari Putusan Coinhive Mahkamah Agung Jepang. Penelitian menggunakan metode penelitian hukum normatif melalui pendekatan peraturan perundang-undangan, kasus, dan perbandingan hukum untuk menganalisis ketentuan hukum siber Indonesia serta pertimbangan hukum dalam putusan tersebut. Berbeda dengan penelitian sebelumnya yang lebih menitikberatkan pada aspek teknis atau pertanggungjawaban pidana, penelitian ini mengembangkan kerangka komparatif yang menempatkan persetujuan pengguna yang sah dan tingkat gangguan terhadap sistem elektronik sebagai parameter utama dalam menentukan pertanggungjawaban pidana. Hasil penelitian menunjukkan bahwa cryptojacking hanya layak dikriminalisasi apabila dilakukan tanpa persetujuan pengguna yang sah serta menimbulkan gangguan yang signifikan terhadap sistem elektronik, eksploitasi sumber daya komputasi pengguna tanpa hak, atau kerugian yang terukur bagi pengguna. Sebaliknya, aktivitas cryptomining yang dilakukan secara transparan berdasarkan perjanjian digital yang sah tidak seharusnya dipandang sebagai tindak pidana karena unsur tanpa hak dan melawan hukum tidak terpenuhi. Penelitian ini berkontribusi terhadap pengembangan hukum pidana siber Indonesia dengan menawarkan parameter normatif yang lebih jelas untuk membedakan cryptomining yang sah dari cryptojacking sebagai tindak pidana melalui prinsip persetujuan pengguna, proporsionalitas, dan penerimaan sosial sebagaimana tercermin dalam Putusan Coinhive.

Kata Kunci

Gangguan sistem elektronik, kriminalisasi, cryptojacking, persetujuan pengguna, putusan coinhive

INTRODUCTION

Over the past decade, human civilization has witnessed dynamic technological advancements, digitalization not only affects conventional economic sectors but also gives rise to new forms of investment based on digital assets, one of which is cryptocurrency. The total market capitalization of cryptocurrencies worldwide was recorded at approximately $3.904 trillion and total transaction in Indonesia reaching IDR 136.31 trillion (InvestorTrust, 2025).

Bitcoin, the first cryptocurrency, was only discovered in 2009 and now cryptocurrency has become one of the most widely used digital investment instruments. The core of this trust lies in the blockchain method, which provides a system of trust in transactions without the need for intermediaries, enabling people to trade valuable items, such as stocks, money, or digital files, with one another (Agung Triayudi, 2025; Budi Raharjo, 2022).

However, behind the innovations offered by cryptocurrency, there are also potential risks. Using a criminological approach through routine activity theory, criminal acts occur when three main elements meet in the same space and time (James Dickety, 2025). Offenders who are motivated to exploit

cyberspace against vulnerable targets, coupled with the state's inability to protect the public, create cybercrime. Cryptocurrency is not only obtained through purchases on digital asset exchanges, but also through the mining process. The mining process is implemented in miner applications for CPUs and GPUs that use JavaScript as the programming language for miner applications because it is supported by most browsers (Michal Salat, 2019).

Digital mining can be done legally with the consent of miners who can use officially registered legitimate providers, providing transparency in services and contracts. However, digital mining can also be done illegally without the consent of users, known as Cryptojacking or Mining Malware (University of Cambridge, 2025). Cryptojacking is very profitable, because the mining proceeds go into the offender's crypto wallet while the victim bears all the costs of mining.

Cryptojacking is a hacking technique in which attackers use other people's devices to mine cryptocurrency without their knowledge or permission (CSIRT UNAIR, 2025). This attack causes CPU/GPU usage to exceed normal limits, infected devices will feel slow and the battery will drain quickly even when used for normal activities. Generally, victims are unaware that their devices have been infected with malware used by perpetrators to mine cryptocurrency (Rüth, Zimmermann, Wolsing, & Hohlfeld, 2018).

The Coinhive case is one of the most prominent examples in the global debate on the legality of cryptojacking. Coinhive provides a JavaScript-based script that automatically instructs visitors' computers to mine Monero without explicit consent (Azizah Binti Abdul Aziz, Syahrulanuar Bin Nga, Yau Ti Dun, & Tan Fui Be, 2020). The Coinhive case in Japan became an important paradigm in cybercrime law after Seiya Moroi, a web designer, was accused in 2017 of violating the Japanese Penal Code for installing a Coinhive script on his website, which authorities considered an unauthorized electronic command violated the Japanese Penal Code (Keita Oda & Yoshiaki Nishigai, 2021). This verdict sparked a global debate about the limits of criminalizing technology that uses users' resources without permission.

Indonesia, as a country governed by the rule of law, has reformed its criminal law through Law No. 1 of 2023 on the Criminal Code (KUHP) by adding provisions on criminal acts related to information technology and electronics (Eddy O. S. Hiariej & Topo Santoso, 2025). Otherwise, in the context of cybercrime, efforts to reform are also being made through a special law, namely Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions. (ITE Law) However, the question arises: how can Indonesia criminal law respond to cryptojacking activities, such as in the Coinhive case?

Existing scholarship provides an important foundation for understanding the legal challenges posed by cryptojacking. Studies may be grouped into three main strands. First, comparative studies examine the criminalization of cryptojacking within specific jurisdictions, such as Hungary, highlighting different legislative approaches to unauthorized cryptocurrency mining

(Gáspár, 2024). Second, Indonesian scholarship primarily focuses on criminal liability for cryptojacking and other cryptocurrency-related offenses within the existing legal framework (Rusmana & Novelin, 2024; Widyatmoko, Atmasasmita, Susanto, & Purwanto, 2024). Third, broader studies on cybercrime discuss the legal implications of cryptocurrency technologies without specifically addressing the normative limits of criminalization in browser-based mining practices.

Despite these contributions, existing studies remain fragmented. Comparative research rarely examines how judicial reasoning shapes the limits of criminal liability, while Indonesian studies generally focus on doctrinal issues without incorporating comparative judicial analysis. Consequently, little attention has been given to the implications of the Japanese Supreme Court's Coinhive Decision for determining when unauthorized cryptomining should be regarded as a criminal offense under Indonesian law. More importantly, previous research has not systematically examined the role of valid user consent and actual harm as normative criteria for limiting criminalization in cases involving browser-based cryptocurrency mining.

Against this background, this article offers a comparative analysis of Indonesian and Japanese law to formulate a proportional framework for assessing criminal liability in cryptojacking cases. Rather than treating every unauthorized use of computing resources as inherently criminal, this study argues that criminalization should depend on two cumulative factors: the absence of valid user consent and the existence of actual harm or significant interference with electronic systems. By incorporating the reasoning of the Coinhive Decision into Indonesian cybercrime discourse, this research extends existing scholarship beyond doctrinal interpretation toward a more balanced framework for determining the boundaries of criminalization.

Accordingly, this article examines whether browser-based cryptocurrency mining without user consent should be criminalized under Indonesian law by drawing lessons from the Japanese Supreme Court's Coinhive Decision. It further evaluates the extent to which the principles developed in that decision can contribute to a more proportional and technology-responsive approach to cybercrime regulation in Indonesia.

This study contributes both theoretically and practically. Theoretically, it enriches cybercrime scholarship by introducing a comparative framework that integrates the concepts of user consent and actual harm as normative limits of criminal liability in unauthorized cryptomining. Practically, it provides guidance for legislators, law enforcement authorities, and policymakers in developing clearer and more proportionate legal standards for addressing emerging forms of cybercrime while avoiding over-criminalization of legitimate technological innovation.

METHOD

This study employs a normative legal research method to examine the limits of criminal liability for unauthorized cryptocurrency mining under

Indonesian law through a comparative legal perspective. The research adopts three complementary approaches. First, the statute approach analyzes the Indonesian Criminal Code (Law No. 1 of 2023), Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law (ITE Law), and relevant provisions of the Japanese Penal Code, particularly Articles 168-2 and 168-3 concerning unauthorized commands to electronic systems. Second, the comparative law approach is used to identify differences and similarities in the criminalization of cryptojacking under Indonesian and Japanese legal systems. Third, the case approach focuses on the Japanese Supreme Court Decision No. 2020 (A) 457 (the Coinhive Decision) to examine its legal reasoning and implications for cybercrime regulation.

The legal materials consist of primary legal sources, including legislation and court decisions, supported by secondary legal materials such as scholarly books, journal articles, and other relevant academic publications on cybercrime, criminal law, and cryptocurrency regulation. All legal materials are analyzed qualitatively using descriptive and comparative legal analysis to evaluate the normative boundaries between lawful browser-based cryptocurrency mining and criminal cryptojacking. Particular attention is given to the concepts of valid user consent, actual harm, and unauthorized use of computing resources as the principal criteria for determining criminal liability under Indonesian cybercrime law.

RESULT AND DISCUSSION

This section discusses the normative limits of criminalizing unauthorized cryptocurrency mining by examining the Japanese Supreme Court's Coinhive Decision and assessing its implications for Indonesian criminal law, particularly regarding the concepts of valid user consent and actual harm.

Chronology and Mechanism of Veiled Mining in the Coinhive Case

Cryptojacking is a type of cyberattack in which attackers secretly use the computing power of victims' computers to mine cryptocurrency without the victims' permission (Varlioglu, Gonen, Ozer, & Bastug, 2020) or use the victim's resources to calculate hashes and profit from mining without the victim's consent (Saad & Mohaisen, 2023). The cryptojacking method used can be carried out by using the attacker's website to place hidden scripts or by placing them on the victim's website (Gáspár, 2024).

The Coinhive case began with the emergence of a browser-based mining service developed by the Coinhive Team in 2017 (Azizah Binti Abdul Aziz dkk., 2020). Initially, this service offered a new monetization model for website owners who previously displayed advertisements/pop-ups. However, through Coinhive, website owners can earn income from mining Monero cryptocurrency by borrowing some of their visitors' computing power (Michal Salat, 2019). Technically, as long as visitors access a website that has Coinhive installed, Coinhive will work through embedded JavaScript. So when the page is opened, the script automatically activates the visitor's device CPU to perform Monero transaction hashing (Rüth dkk., 2018).

Visitors' devices are essentially unaware that they have been infected by Coinhive or cryptojacking, as there is no software installation, no notification, and mining continues as long as the tab remains open. The results of these calculations are then sent to the Coinhive server, and the crypto rewards are divided between the Coinhive service provider and the site administrator (Keita Oda & Yoshiaki Nishigai, 2021).

Analysis of the Japanese Court's Verdict in the Coinhive Case

One of the most prominent Coinhive cases in Japan involved Seiya Moroi, a web designer who managed a music sharing site for using the Coinhive program to mine cryptocurrency (The Asahi Shimbun, 2022). Seiya Moroi will receive 70% of the mining revenue, while Coinhive will receive 30%. In 2017, Seiya Moroi installed the Coinhive script on the website he managed, intending to generate revenue to keep the site operational (Mainichi Daily News, 2022). The script automatically utilizes visitors' devices to mine Monero without notification or explicit consent from users.

An interesting point in the case of Seiya Moroi, Yokohama District Verdict, March 27, 2019, No. 2446, was that the court found that the offender did not act intentionally but did not find any fault, and acquitted Seiya Moroi (Keita Oda & Yoshiaki Nishigai, 2021). The prosecutor appealed and argued that the Coinhive script was a program that executed commands contrary to the user's will and was illegal because it was used without consent. Subsequently, on February 7, 2020, the Tokyo High Court, Hanrei Jiho No. 2446, ruled differently, sentencing Seiya Moroi to a fine of ¥100,000 for violating Articles 168-2 and 168-3 of the Japanese Penal Code regarding the storage of electronic or magnetic records containing illegal commands (Supreme Court Japan, 2022). This prompted Seiya Moroi to file a lawsuit with the Japanese Supreme Court to obtain legal certainty regarding the criminal status of using Coinhive.

The second-instance verdict was subsequently overturned by the Japanese Supreme Court in its verdict on Case No. 2020(A)457, which became a crucial point in the development of Japanese cybercrime law, including how Coinhive is viewed. The Japanese Supreme Court not only assessed the factual aspects of the act, but also formulated a normative standard to determine whether a program can be classified as "electronic or magnetic records" for which the Japanese Criminal Code provides criminal sanctions for the creation and provision of "Improper Command Records", namely records that give improper commands to a computer, such as computer viruses (fusei shirei denji-teki kiroku) (Hamada, 2025; Keita Oda & Yoshiaki Nishigai, 2021). The considerations given by the Supreme Court of Japan are as follows (Supreme Court Japan, 2022) a) The elements of the offense are cumulative; b) Coinhive contradicts the user's wishes because there is no notification or consent; c) The standard for "Improper Command Records" is determined by social acceptance; d) The technical impact of Coinhive is considered minimal and acceptable due to its limited CPU usage.

Under Article 168-2 of the Japanese Penal Code, any person who, without justifiable grounds, creates or provides an Improper Command Records, or intentionally infects or attempts to infect a computer with such a records, shall be punished by imprisonment for up to three years or a fine of up to 500,000 yen (Hamada, 2025). Various forms of malware, such as ransomware, spyware, worms, trojans, and other computer viruses, are consistently classified as Improper Command Records and are punishable as cybercrimes.

According to Japanese criminal law, criminal liability for cybercrime in the Coinhive case is not based solely on the concepts of "loss" or "illegal access," but rather on the specific offense of fusei shirei denjiteki kiroku (electronic or magnetic containing improper command records) as stipulated in Articles 168-2 and 168-3 of the Japanese Penal Code (Keita Oda & Yoshiaki Nishigai, 2021). Criminal liability does not automatically arise simply because a program runs without the user's explicit consent, but must fulfill two cumulative elements, as follows (1) the nature of being contrary to the user's will (anti-intentionality) and (2) the nature of being an "Improper command" (illegitimacy), which is determined through social acceptance standards.

The Japanese Supreme Court, in the case of Seiya Moroi, affirmed that criminal liability under Article 168-2 paragraph (1) of the Japanese Criminal Code requires the fulfillment of two cumulative elements, namely the existence of an order that is contrary to the will of the user and the "illegal" nature of the order. The first element is assessed normatively based on the function of the program as it should be recognized by the general user, not based on technical awareness or the subjectivity of individual users (Supreme Court Japan, 2022). Japanese criminal law seeks to avoid expanding criminalization to complex and dynamic technological practices.

In the Coinhive case, the Japanese Supreme Court ruled that the element of "opposite to the user's will" was fulfilled. As a result, users cannot reasonably anticipate that their devices will be used for crypto mining, so the actual function of the program differs from the function that users normatively assume when accessing the website (Keita Oda & Yoshiaki Nishigai, 2021).

However, the Japanese Supreme Court rejected the element of "improper command records". This element was assessed using social acceptance standards, the Japanese Supreme Court considered the level of technical impact on users' computers, the methods of using the program, and its comparison with other monetization mechanisms that are socially acceptable, such as digital advertising (Mainichi Daily News, 2022).

This approach by the Japanese Supreme Court reflects caution in the use of criminal law as an instrument of technological control. Emphasizing the placement of social acceptance standards (shakai tsūnen) as the main filter, criminal law is positioned as an ultimum remedium and is not used to respond to every non-transparent technological practice.

Shakai tsūnen is a concept of judicial reasoning used in Japanese law, referring to a judge's perception of the sense of justice, values, and fairness that

exist in society (Haley, 2011). Although this concept is not clearly defined, it serves as a social benchmark for assessing whether an act or legal consequence is socially acceptable.

With shakai tsūnen, Japanese judges tend to take a communitarian approach that emphasizes harmony, consensus, and legal stability, while avoiding absolute moral judgments. Although this approach provides legal certainty and prevents excessive criminalization, this ruling shows that user protection in the context of cryptojacking is more directed towards non-criminal regulation, such as transparency obligations and digital consumer protection.

Analysis of the Japanese Court's Verdict in the Coinhive Case Liability for Cryptojacking Mining under Indonesian Criminal Law

Cryptocurrency is defined as a commodity asset that can be traded (I Made Dwipa Anggara Putra Duwalang & Dewa Gede Pradnya Yustiawan, 2025). Cryptojacking is essentially the act of utilising other people's computing resources without their consent in order to gain economic benefit (Varlioglu dkk., 2020). Indonesian criminal law does not explicitly regulate this as a criminal offence, but it can be categorised as a concurrence of offences (concursus idealis) because one act fulfils several provisions of the law, as stipulated in Article 125 of the Criminal Code (Eddy O. S. Hiariej & Topo Santoso, 2025). Therefore, based on the analysis, cryptocurrency mining in Indonesia will result in the following two conditions:

1. Not a Criminal Act

Crypto mining cannot be criminalised if it is carried out transparently and with the user's consent. The main element of the offence in Article 30 of the ITE Law or Article 34 of the ITE Law or Article 36 of the ITE Law or Article 332 of the Criminal Code, namely the element of 'without rights' or 'against the law', may not be fulfilled when users are aware that some of their computing resources are being used for cryptocurrency mining through the terms and conditions agreed to by the users.

The terms and conditions of the smart contract (T&C) agreed to by users on digital platforms constitute a valid and legally binding agreement (Möslein, 2023), which creates a digital contract between the platform provider and the user. Normatively, digital contracts are recognised as valid agreements as long as they meet the requirements for a valid agreement as stipulated in Article 1320 of the Indonesian Civil Code, namely agreement between the parties, competence, a specific object, and a lawful cause. User consent through click-wrap or sign-in wrap agreement mechanisms has been understood as a valid intention in modern civil law (Morae, 2023) and global platform practices. Thus, if crypto mining is explicitly stated in the T&Cs and agreed to by the user, or if the user does not read carefully but gives their consent, then a legal relationship has been established that is consensual and valid and does not constitute unilateral exploitation.

User-consent-based crypto mining is a legitimate alternative form of digital monetisation that is comparable to the advertising model (pop-ups). Thus, access to electronic systems/computing resources is lawful and does not violate the legal interests of the system owner's exclusive rights to their computer. Furthermore, this activity cannot be criminalised because the use of users' computing resources is accompanied by a benefit-sharing mechanism that has been contractually agreed upon. The mutually beneficial relationship is quid pro quo in nature.

Based on Jed Lewinsohn, in the ordinary quid pro quo exchange, each party agrees to do their part to get the other party to do theirs; each conditions their own willingness to perform on the willingness of the other (Lewinsohn, 2019). Users consciously agree that part of their CPU capacity or computing power will be used for crypto mining and, in return, will receive certain benefits in the form of crypto profit sharing, access to premium services, removal of advertisements, or continuity of digital services.

However, the nature of the T&C or user agreement as a justification is not absolute. User consent is only binding if the substance of the agreement does not breach the objective requirements of Article 1320 of the Civil Code, particularly regarding lawful cause. Contractual clauses that are misleading, non-transparent, or substantially exploit users have the potential to violate the principles of public order and good faith and may therefore be declared null and void. If consent is also obtained through manipulation or technical deception, the digital contract will lose its legal relationship because it may be declared null and void, and the act may again be classified as an unlawful act.

Using a criminal liability approach, this condition does not indicate any fault (schuld) that can be held criminally liable (Albert Aries, 2024). User consent removes the illegal nature of crypto mining, as the use of computing resources occurs within a voluntary and contractual legal relationship. This highlights the importance of understanding the T&C before giving consent.

The receipt of benefits by users reinforces the absence of fault (schuld) and unlawfulness in criminal liability. The perpetrator not only acts with permission but also provides a transparent and predictable distribution of benefits to users. Thus, this type of crypto mining cannot be equated with cryptojacking, in which the perpetrator unilaterally takes advantage by burdening the victim's system without their knowledge or compensation.

Users will not suffer losses, thus fulfilling the purpose of criminal law, which is to protect electronic systems and freedom from harmful abuse. However, when users obtain real and proportional benefits as agreed in the T&C, there is no violation of these legal interests. Conversely, if they do not obtain real or proportional benefits in the T&C, then an unlawful act under civil law has occurred.

Furthermore, the application of Articles 30, 34, and 36 of the ITE Law and Article 332 of the Criminal Code requires the element of "without rights" or "against the law," which is an objective element and must be proven,

including the element of intent. When consent is given legally through a digital contractual mechanism, this element is automatically not fulfilled. This is because an act can only be classified as a criminal offense if it fulfills all elements of the offense and violates protected legal interests tangibly. The use of computing resources occurs within the framework of a legal relationship that is valid and voluntarily agreed upon, so it cannot be considered a form of seizure, intrusion, or misuse of electronic systems, but is similar to digital advertising models or user-permission-based data processing that has been widely accepted in global practice.

2. Criminal Act

Crypto mining can be criminalized if it is carried out veiledly without the knowledge and consent of users, which is a criminal offense in the form of a violation of regulations. In this case, the practice of cryptojacking clearly fulfills the elements of "unauthorized or unlawful access to another person's computer or electronic system" as stipulated in Article 30 of the ITE Law and Article 332 of the Criminal Code.

The element of "everyone" is fulfilled because the legal subjects in cryptojacking practices can be individuals, groups, or digital platform managers. The element of "intentionally" is reflected in the active act of embedding crypto mining scripts or codes into users' systems, which is done consciously and deliberately to obtain economic benefits. This intent does not have to be proven through malicious intent, but rather through the offender's knowledge and will that another person's electronic system will be used without permission, which is a form of conscious intent.

The element of "without rights or against the law" is central to criminal liability in cryptojacking cases. In cryptojacking, there is no user consent, either explicit or implicit, through digital contract mechanisms (T&C). The absence of consent removes the legal basis for perpetrators to utilize the victim's computing resources. Thus, the use of the user's CPU, memory, and electrical power for crypto mining purposes is automatically unlawful. This distinguishes cryptojacking from legitimate crypto mining, where the use of resources is based on consent and a valid legal relationship.

Furthermore, the element of "accessing a computer or electronic system" in Article 30 of the ITE Law and Article 332 of the Criminal Code is not interpreted narrowly as merely entering the system but also includes the use of internal functions of the electronic system. When performing cryptojacking, the offender not only "enters" the system but also controls some of the computing functions of the user's device to perform crypto hashing. Such access clearly exceeds the owner's intent and control, thereby meeting the criteria for illegal access. Therefore, crypto mining conducted veiledly without the user's consent can be held criminally liable under Article 30 of the ITE Law and Article 332 of the Criminal Code, both as an illegal access offense and as part of a cybercrime oriented toward obtaining economic gain unlawfully.

Furthermore, parties that produce, provide, or distribute software specifically designed for cryptojacking may be subject to Article 34 of the ITE Law because their actions directly facilitate illegal access and disruption of electronic systems (Republik Indonesia, 2024). Article 34 paragraph (1) of the ITE Law criminalizes the act of producing, selling, procuring for use, importing, distributing, providing, or possessing hardware or software that is designed or specifically developed to facilitate the acts referred to in Articles 27 to 33 of the ITE Law (Republik Indonesia, 2024). The elements of "everyone" and "intentionally" are fulfilled when the offender consciously creates or distributes cryptojacking software with the intention of running it on another party's electronic system. This intent does not have to be proven through explicit malicious intent, but rather through the awareness that the software will be used to access or utilize electronic systems without authorization.

The term "software that is designed or specifically developed" means that crypto mining scripts or malware are generally created with certain technical characteristics, such as running hidden, utilizing the user's CPU or GPU, and sending the hashing results to the offender's server without the user's consent. Therefore, cryptojacking software qualifies as a means that is technically and functionally developed to commit illegal acts.

Furthermore, the element of "facilitating the acts referred to in Articles 27 to 33" of the ITE Law can be fulfilled because cryptojacking directly enables illegal access (Article 30 of the ITE Law) and in many cases causes disruption to electronic systems (Article 33 of the ITE Law), such as increased CPU load, excessive power consumption, decreased performance, or system instability. Thus, criminal liability under Article 34 of the ITE Law is not only directed at offenders who carry out cryptojacking, but also at parties who act as creators, providers, or distributors of cryptojacking malware. This confirms that under Indonesia's cyber criminal law regime, cryptojacking is considered a criminal offense based on the theory of the functioning of tools.

The occurrence of disturbances to the user's electronic system, such as increased CPU load, power consumption, decreased device performance, or even system damage, constitutes a relevant legal consequence for the application of Article 33 of the ITE Law. Article 33 of the ITE Law requires any act that results in the disruption of an Electronic System and/or causes the Electronic System to not function properly (Republik Indonesia, 2024).

The elements of intent and without rights or against the law are fulfilled in the practice of cryptojacking because the perpetrator consciously implants crypto mining code or scripts into the victim's electronic system to utilize computing resources without the will or consent of the user, including the use of the device's CPU, memory, and electricity. The consequences of cryptojacking clearly fulfill the element of "disruption of Electronic Systems," as this practice causes increased CPU load, excessive power consumption, decreased device performance, overheating, and potential long-term system damage. Although such disruptions do not always cause the system to shut down completely,

Article 33 of the ITE Law does not require permanent damage, but rather the existence of conditions in which the system does not function properly.

This punishment may also be imposed if the proceeds from crypto mining obtained from the use of the user's computing resources are partially or wholly taken by the offender. In this case, cryptojacking is not limited to illegal access and the creation of malware but also has the potential to be classified as an act similar to economic theft. Given that cryptocurrency is recognized as a tradable asset or commodity, the unauthorized appropriation of mining proceeds can be analyzed as the appropriation of intangible "goods" or as the unauthorized transfer of Electronic Information as referred to in Article 32 paragraph (2) of the ITE Law or theft in its basic form as referred to in Article 476 of the Criminal Code. Thus, cryptojacking is no longer merely a technical system violation but a criminal act that directly harms the economic interests of the victim.

Based on the overall analysis and conditions above, it can be confirmed that determining whether or not to prosecute cryptojacking does not focus on the act of crypto mining as a technology, but rather on the legality of access, transparency of mechanisms, and the existence of user consent. Indonesian criminal law, through the ITE Law and the Criminal Code, consistently requires the element of "without rights" or "against the law" as the main basis for criminal prosecution. Therefore, if the use of computing resources is carried out legally and based on consent, it is not subject to criminal law.

This analysis also emphasizes the urgency of the ultimum remedium principle in cyber criminal law. The use of criminal law against digital activities that are still in a regulatory gray area risk creating legal uncertainty and hindering innovation, which is contrary to the principles of lex certa, lex scripta, and lex stricta in the principle of legality. Therefore, criminal prosecution for cryptojacking should only be pursued if the act truly violates user rights or causes harm/violates interests or is unlawful/unauthorized.

When a script programmed as malware is executed without consent, infiltrates the user's system, and exploits computing resources for the offender's benefit, then such an act normatively violates the legal interests protected by the ITE Law and the Criminal Code. Cryptojacking cannot be viewed as merely an alternative monetization practice, but rather as a form of criminal misuse of technology.

Thus, the dividing line between acts that are not criminal and those that are criminal must be normatively defined: transparency and consent negate the unlawful nature of an act, while concealment, unauthorized use, and unilateral profit-taking form the basis for criminal liability. This clarification is not only important for legal certainty but also provides direction for the reform of cyber criminal law in Indonesia to be more adaptive to technological developments.

Analysis of the Japanese Court's Verdict in the Coinhive Case Liability for Cryptojacking Mining under Indonesian Criminal Law

A comparison between the Japanese and Indonesian legal approaches

to cryptojacking reveals fundamental differences in the role of criminal law in responding to technological developments.

Japan, through the Supreme Court verdict in the Coinhive case, adopted a cautious and contextual approach by prioritizing the element of social acceptance (shakai tsūnen), considering the technical impact, and the purpose of using technology as the main parameters of criminal liability. This approach emphasizes that not every act that is contrary to the will or harmful to users is automatically classified as a criminal offense.

In contrast, Indonesian criminal law, through the ITE Law and the Criminal Code, tends to use broad and formal formulations of offenses, particularly emphasizing the elements of "without rights" and "against the law." This formulation indicates strong law enforcement against harmful cryptojacking practices without considering whether the impact is low or high as long as it meets the provisions of the law.

The Japanese Supreme Court verdict provides a different paradigm in considering that user consent should be positioned as a central factor in assessing the unlawful nature of an act. Crypto mining conducted transparently through digital contracts that are valid, understood, and agreed upon by users should not be criminalized because the element of "without rights" is not fulfilled. In addition, Japan emphasizes the importance of the standard of actual impact on electronic systems. The Japanese Supreme Court ruled that the use of a small portion of CPU resources that does not cause significant disruption to computer performance is not sufficient to qualify a program as an "improper command" This approach is relevant to Indonesia, which still needs objective parameters regarding what constitutes "disruption of electronic systems" in Article 33 of the ITE Law, so that criminalization is not based solely on technical assumptions without actual losses.

Indonesian criminal law needs to clarify the normative boundaries between legal crypto mining and cryptojacking by emphasizing that valid user consent through digital contracts eliminates the elements of "unauthorized" and "illegal," as long as there is no fraud, technical manipulation, or violation of valid agreement terms, or if there is a growing phenomenon, special regulations can be made against crypto abuse. This clarity is important to prevent overcriminalization and increase legal certainty in the digital economy ecosystem. In addition, the enforcement of cyber criminal law should require proof of actual and significant interference with electronic systems, not just potential or technical assumptions, so that criminal law functions as an ultimum remedium.

The author further argues that user consent should constitute the primary criterion in distinguishing lawful cryptomining from criminal cryptojacking. Where users have provided informed and valid consent through transparent digital agreements, the elements of unlawfulness and lack of authorization should generally be considered absent, unless such consent was obtained through fraud, deception, or technical manipulation. This approach is consistent with the principle of legal certainty and prevents criminal law

from inhibiting legitimate technological innovation.

From a law reform perspective, Indonesia should adopt clearer statutory standards regarding the meaning of "electronic system disruption" under Article 33 of the ITE Law. Criminal liability should require proof of actual and significant interference with system performance rather than merely hypothetical risks or technical assumptions. Such a reform would align cybercrime regulation with the principle of *ultimum remedium*, ensuring that criminal sanctions are reserved for conduct that causes genuine harm.

Accordingly, the author proposes that future cybercriminal law reform in Indonesia incorporate several principles reflected in the Coinhive decision: (1) recognition of informed user consent as a key determinant of legality; (2) the establishment of objective thresholds for assessing system interference and harm; and (3) the limitation of criminalization to conduct that produces significant adverse effects on users or electronic systems. These reforms would strengthen legal certainty while allowing criminal law to remain adaptive to technological developments and digital economic activities.

CONCLUSION

This research confirms that criminal liability for cryptojacking depends primarily on the existence of valid user consent and the degree of interference with electronic systems. The Japanese Supreme Court's Coinhive Decision demonstrates that the use of computing resources without explicit consent should not automatically be classified as a criminal offense where it does not cause significant disruption to electronic systems and remains within the limits of social acceptance (shakai tsūnen). This finding suggests that an overly expansive approach to criminalization may create legal uncertainty and discourage technological innovation. In the Indonesian context, cryptojacking should be criminalized where it is carried out without valid user consent and results in significant interference with electronic systems, unauthorized exploitation of computing resources, or other measurable harm to users. Conversely, crypto mining conducted transparently with informed user consent and without causing substantial disruption should not attract criminal liability because the elements of unlawfulness and unauthorized conduct are absent. Accordingly, the normative boundary between lawful cryptomining and criminal cryptojacking should be determined primarily by two factors: valid user consent and significant interference with electronic systems. This study contributes to Indonesian cybercriminal law by proposing clearer normative parameters for distinguishing lawful cryptomining from criminal cryptojacking. It recommends that Indonesian law move beyond a purely formal interpretation of the elements of "without rights" and "against the law" by giving greater consideration to informed user consent, significant system interference, and the principle of social acceptance (shakai tsūnen) reflected in the Coinhive Decision. These principles may provide a more adaptive, proportionate, and technology-responsive framework for future cybercrime regulation.

REFERENCES

Aries, A. (2024). *Hukum pidana Indonesia menurut KUHP lama & KUHP baru* (Edisi ke-1). Depok: PT Rajagrafindo Persada.

Azizah, B. A. A., Nga, S. B., Dun, Y. T., & Be, T. F. (2020). Coinhive's Monero drive-by crypto-jacking. *IOP Conference Series: Materials Science and Engineering*. Makalah dipresentasikan pada The 6th International Conference on Software Engineering & Computer Systems. https://doi.org/10.1088/1757-899X/769/1/012065

CSIRT UNAIR. (2025, Januari 22). *Cryptojacking: Malware penambangan kripto secara ilegal*. Diambil dari https://csirt.unair.ac.id/cryptojacking-malware-penambangan-kripto-secara-ilegal/

Dickety, J. (2025). *Criminology and crime prevention* (Vol. 2). New York: Routledge.

Duwalang, I M. D. A. P., & Yustiawan, D. G. P. (2025). Pengaturan hak waris atas aset digital dalam perspektif asas kepastian hukum. *Jurnal Media Akademik*, *3*. https://doi.org/10.62881

Gáspár, Z. (2024). The criminalization of cryptojacking in Hungary. *Problemy Prawa Karnego*, *8*(2), 1–16. https://doi.org/10.31261/PPK.2024.08.02.01

Haley, J. O. (2011). Constitutional adjudication in Japan: Context, structures, and values. *John Owen Haley*, *88*(6), 1467–1491.

Hamada, M. (2025, November 21). *International comparative legal guides*. Diambil dari https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan

Hiariej, E. O. S., & Santoso, T. (2025). *Anotasi KUHP nasional*. Depok: PT Rajagrafindo Persada.

InvestorTrust. (2025, Oktober 21). *Transaksi kripto di pasar derivatif Indonesia melonjak 118% di kuartal III 2025 tembus Rp 52,71 triliun*. Diambil dari https://investortrust.id/market/82860/transaksi-kripto-di-pasar-derivatif-indonesia-melonjak-118-di-kuartal-iii-2025-tembus-rp-52-71-triliun

Lewinsohn, J. (2019). Paid on both sides: Quid pro quo exchange and the doctrine of consideration. *SSRN Electronic Journal*, 690–772. https://doi.org/10.2139/ssrn.3471850

Mainichi Daily News. (2022, Januari 21). Japan's top court clears man accused of cryptocurrency mining without users' consent. *Mainichi Daily News*. Diambil dari https://mainichi.jp/english/articles/20220121/p2a/00m/0na/013000c

Morae. (2023, April 12). *Clickwrap agreements: Everything you need to know*. Diambil dari https://www.morae.com/insights/clickwrap-agreements/

Möslein, F. (2023). Digitized terms: The regulation of standard contract terms in the digital age. *European Review of Contract Law*, *19*(4), 300–320. https://doi.org/10.1515/ercl-2023-2019

Oda, K., & Nishigai, Y. (2021). A study of crimes related to electronic or magnetic records containing unauthorized commands based on practice

of application development. *Chiba Association of Law and Politics*, *36*(1), 56. https://doi.org/10.20776/S09127208-36-1-P056

Raharjo, B. (2022). *Uang masa depan: Blockchain, Bitcoin, cryptocurrencies*. Semarang: Yayasan Prima Agus Teknik.

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905.

Rusmana, I. P. E., & Novelin, T. (2024). Legal analysis of criminal responsibility for hackers from the perspective of cyber law in Indonesia. *JIHAD: Jurnal Ilmu Hukum dan Administrasi*. https://doi.org/10.58258/jihad.v6i4.7676

Rüth, J., Zimmermann, T., Wolsing, K., & Hohlfeld, O. (2018). Digging into browser-based crypto mining. *Proceedings of the Internet Measurement Conference 2018*, 70–76. https://doi.org/10.1145/3278532.3278539

Saad, M., & Mohaisen, D. A. (2023). Analyzing in-browser cryptojacking. *IEEE Transactions on Dependable and Secure Computing*, *21*, 5448–5460. https://doi.org/10.1109/tdsc.2024.3377533

Salat, M. (2019, Maret 8). *The end of Coinhive; The end of cryptojacking?* Diambil dari https://blog.avast.com/coinhive-shuts-down

Supreme Court Japan. (2022, Januari 20). *Judgments of the Supreme Court*. Diambil dari https://www.courts.go.jp/english/Judgments/search/1882/index.html

The Asahi Shimbun. (2022, Januari 21). *Website owner not guilty over nonconsensual bitcoin mining*. Diambil dari https://www.asahi.com/ajw/articles/14527143

Triayudi, A. (2025). *Blockchain* (Edisi ke-1). Yogyakarta: PT Penamuda Media.

University of Cambridge. (2025). *Cambridge digital mining industry report*. Cambridge: University of Cambridge. Diambil dari https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf

Varlioglu, S., Gonen, B., Ozer, M., & Bastug, M. F. (2020). Is cryptojacking dead after Coinhive shutdown? *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, 385–389. https://doi.org/10.1109/ICICT50521.2020.00068

Widyatmoko, U., Atmasasmita, R., Susanto, A. F., & Purwanto, B. H. (2024). Law enforcement against cryptocurrency abuse. *Journal of Social Research*. https://doi.org/10.55324/josr.v3i2.1941