

Problems of Qualification of Criminal Offenses in the Sphere of Crypto-Assets Turnover and Mining

Bakhtiyor Primov,^{1*}

¹ Academy of Justice of the Republic of Uzbekistan

*baxti13051993@gmail.com

DECLARATIONS

Ethical Statement:

This research was conducted in accordance with the COPE Core Practices and principles of academic integrity, transparency, and responsible research.

Data Availability Statement:

Data supporting this study are available from the corresponding author upon reasonable request, where applicable.

AI Declaration:

The authors acknowledge the use of AI tools in conducting and preparing this research and remain fully responsible for its content, accuracy, and originality.

Conflict of Interest Statement:

The authors declare no conflicts of interest.

Funding Statement:

The authors received no funding for this research.



This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction provided the original work is properly cited.

Abstract

Crypto-assets have created new opportunities for crime that existing criminal codes struggle to classify. Bribes, laundered funds, and stolen computing power now move through block chain networks. This study aims to examine problems of criminal qualification in crypto-assets turnover and mining. It seeks to identify gaps in offence definitions and propose a coherent liability model. The research adopts a qualitative design based on doctrinal and document analysis. It reviews Uzbek legislation, European Union regulations, Russian law, and scholarly literature. The results show that the unclear legal status of tokens weakens property and bribery offences. Laundering through mixers and non-fungible tokens escapes traditional definitions. Crypto jacking lacks a clear offence category, while illegal mining harms energy security and the environment. The study recommends recognizing crypto-assets as property for criminal purposes. It also proposes specific offences for crypt jacking and large-scale illegal mining. Clear rules would strengthen deterrence, protect victims, and support lawful digital innovation.

Keywords: Crypto-Assets, Criminal Qualification, Crypto jacking, Illegal Mining, Money Laundering, Bribery, Non-Fungible Tokens

How to Use Cite (APA 7th Edition)

Primov, B. (2026). Problems of Qualification of Criminal Offenses in the Sphere of Crypto-Assets Turnover and Mining. *Uzbek Journal of Law and Digital Policy*, 4(5), 260-279. <https://doi.org/10.59022/IRSHAD-ujldp.14>

Authors Contribution:

Full.

I. INTRODUCTION

Criminals now move illicit money across borders in seconds using digital currencies. This speed has changed how crime is planned, committed, and concealed worldwide. Crypto currency promised financial freedom, yet it also opened new doors for offenders. Bribes, laundered funds, and stolen computing power now travel through block chain networks. Traditional criminal law was written for cash, banks, and physical property alone. Courts and prosecutors struggle to fit digital assets into these old legal categories. This mismatch allows many offenders to escape liability through technical legal loopholes. The issue matters because public trust in financial systems depends on effective enforcement. It also matters because victims often lose savings without any clear legal remedy. This article examines how criminal law should respond to crimes involving crypto-assets. It asks whether existing offences are adequate or whether new legal rules are needed. Organized criminal groups already exploit these assets for profit and secrecy (Arnone, 2025).

Bit coin appeared in 2009 as a peer-to-peer system without any central authority. Early users valued its privacy and its freedom from state control. Criminals soon noticed the same features and used them on dark net markets. The Silk Road case showed how digital coins could fund illegal drug sales. Law enforcement agencies later learned that public block chain records could also trace suspicious payments. States then responded by extending anti-money laundering rules to virtual asset providers. The Financial Action Task Force issued guidance requiring exchanges to identify their customers. Many countries also introduced licensing systems for crypto exchanges and wallet services. These steps improved oversight, but they focused mainly on regulation, not criminal liability. Scholars studied financial stability and compliance more than the definition of crypto offences. Questions about bribery, mining harm, and token-based laundering received limited attention. Existing research shows that preventive measures alone cannot remove crypto-related financial risk (Antwi, 2023).

We already know that crypto-assets are widely used in serious financial crime. We also know that regulators have built compliance duties for exchanges and wallets. The legal status of crypto-assets in criminal law remains uncertain in many countries. Some laws treat them as property, while others treat them as mere digital information. This uncertainty creates problems when courts must decide whether a crime has occurred. A bribe paid in tokens may not fit the statutory meaning of property. Laundering through non-fungible tokens may escape rules designed for traditional financial assets. Hidden mining on another person's computer may not match classic theft or damage offences. The exact problem is the gap between crypto-related conduct and existing offence definitions. We still need to know how criminal law should classify, prove, and punish such harmful conduct in practice. Courts face real difficulty when deciding whether crypto currency can serve as a bribe (Ageev, 2025).

Recent studies show growing concern about crypto-assets in organized financial crime. Research from 2023 linked weak anti-money laundering controls with wider financial sec-

tor instability. Studies in 2025 examined how criminal groups exploit digital coins for secrecy. These works confirm that crypto misuse is no longer a marginal criminal practice. Attention has also shifted toward newer assets such as non-fungible tokens. Non-fungible tokens allow criminals to inflate prices through fake sales between linked accounts. Prices of such tokens are subjective, so unusual sales rarely raise suspicion. This method turns illegal funds into apparently lawful profits from digital art. Terrorist groups may also use such tokens to receive funds across borders quietly. Many national laws do not clearly cover these tokens within money laundering offences. This weakness makes prosecution difficult and allows offenders to exploit legal uncertainty. Recent research calls for clear criminal liability rules for laundering through non-fungible tokens (Al-Balushi, 2025).

A second line of research studies crimes committed against computing resources. Crypto jacking means secretly using another person's device to mine digital coins. Attackers often hide malicious mining code inside popular websites, mobile applications, or cloud servers. Victims rarely notice this conduct because nothing appears to be stolen from them. Their devices slow down, consume more electricity, and suffer faster physical wear. Some legal systems treat this conduct as unauthorized access to an information system. Others prefer to classify it as theft of electricity or damage to property. These different approaches create inconsistent outcomes for similar harmful conduct. Scholars also note that sentencing remains weak because the harm seems small. Victims across many devices may still suffer large combined losses from such attacks. Comparative research remains necessary to build a coherent criminal law response across jurisdictions. A Hungarian study shows how one country has criminalized crypto jacking through specific provisions (Gáspár, 2024).

The literature has clear strengths in describing how criminals misuse crypto-assets. It explains laundering techniques, bribery risks, and the threat of hidden mining. Most studies examine one offence or one country in isolation from others. Few works build a single framework that connects all crypto-related offences together. The literature also focuses heavily on compliance duties rather than core criminal liability. Questions about men's rea, harm, and the property status of tokens remain unsettled. Empirical data on prosecutions and convictions for crypto offences remains limited. Environmental harm from mining has only recently entered criminal law debates. Many authors suggest future research on unified offence definitions and comparative reform. No current study combines bribery, laundering, fraud, and mining within one legal model. This article fills that gap through a comparative and doctrinal analysis of crypto offences. Scholars now argue that criminal law reform must also address energy harm from mining (Fernando, 2025).

To examine how existing criminal law classifies crypto-assets in bribery, money laundering, fraud, and crypto jacking offences.

To identify gaps and inconsistencies in current offence definitions across selected legal systems.

To propose a coherent legal framework for criminal liability in crypto-related offences.

How can criminal law redefine its offence categories to impose coherent liability for bribery, money laundering, fraud, and crypto jacking involving crypto-assets?

This study is needed because crypto crime grows faster than criminal law reform. It offers lawmakers a clear model for defining crypto-related offences in statutes. Judges may use its findings to classify tokens consistently in bribery and laundering cases. Prosecutors may gain stronger tools to charge offenders who exploit legal loopholes. Victims may benefit from clearer liability rules and better chances of recovering their stolen digital assets. The study also adds new knowledge by connecting separate offences within one framework. Academics can test this framework in other legal systems and emerging technologies. Financial institutions may use it to align compliance programmers with criminal law duties. Society benefits when digital markets become safer and more trustworthy for ordinary users and investors. This contribution matters because courts already stretch old offences to reach crypto misconduct. Prosecutors in the United States have even used wire fraud law against crypto insider trading (Balaji, 2023).

II. METHODS & METHODOLOGY

This study adopted a purely qualitative research design to examine criminal qualification problems involving crypto-assets. The qualitative approach suits legal research because it focuses on meaning, wording, and interpretation. The study relied on doctrinal analysis to examine statutes, court judgments, and official legal guidance. Document analysis was used to review scholarly articles, policy papers, and regulatory reports. The legal sources included the Criminal Code of the Republic of Uzbekistan and its recent amendments. Presidential Decree No. PP-3832 of 2018 on the development of the digital economy was also examined. Foreign sources included the European Union Markets in Crypto-Assets Regulation and Transfer of Funds Regulation. The Criminal Code of the Russian Federation and its Law on Digital Financial Assets were reviewed. International instruments included the Convention on Cybercrime and the United Nations Convention against Corruption. These sources allowed comparison of how different systems treat crypto-related bribery, laundering, crypt jacking, and illegal mining.

Legal texts were collected only from official government and institutional web portals. Uzbek legislation was retrieved from the national legal database at lex.uz. European Union instruments were obtained from the official EUR-Lex portal. Russian laws were taken from the official legal information portal of the Russian Federation. International standards were collected from official United Nations and Financial Action Task Force websites. The search used keywords such as crypto-assets, criminal qualification, crypt jacking, and illegal mining. Additional keywords included crypto bribery, virtual assets, money laundering, and non-fungible tokens. Only peer-reviewed law and criminology journals with digital object identifiers were selected. Most selected articles were published within the last five years to ensure relevance. Only laws currently in force were analyzed to maintain the validity and reliability of findings.

The study used only official documents and scholarly sources available in the public domain. No human participants, interviews, or questionnaires were involved at any stage of this research. Every scholarly article used in this study is properly cited in the reference list. This practice respects the original authors and maintains academic integrity throughout the paper. The researcher has no conflict of interest, and the study serves purely academic purposes. The study also has certain natural boundaries that readers should keep in mind. It focused mainly on Uzbekistan, with selected comparisons from the European Union, Russia, and Japan. It examined only bribery, money laundering, fraud, crypt jacking, and illegal mining offences. Crypto technology evolves rapidly by nature, and new token types appear almost every year. Laws and regulations in this field can also be amended at any time. Some findings may need updating as legislators respond to new forms of crypto-related crime.

III. RESULTS& FINDINGS

This section presents the main findings on crypto-assets turnover and mining offences. The study examined how criminal law qualifies conduct involving digital tokens and mining. It followed the research question on coherent liability for crypto-related offences. The analysis covered bribery, money laundering, fraud, crypto jacking, and illegal mining farms. Each area was tested against existing offence definitions in selected legal systems. The aim was to find where current rules fail to capture harmful conduct. Court practice, statutory texts, and recent scholarship formed the basis of this analysis. The findings reveal that most problems begin with the uncertain legal status of tokens. They also show that offenders exploit gaps between technology and legal definitions. Each result connects directly to one or more research objectives stated earlier. These results explain why current qualification practice remains inconsistent and weak. The threats are not only digital, since offenders also attack crypto holders physically (Ordekian, 2024).

The unclear legal status of crypto-assets is the root problem of criminal qualification. Many criminal codes do not state whether crypto-assets count as property. Some courts treat tokens as property, while others treat them as digital information. Judges in the same country sometimes reach opposite conclusions on identical facts. This split affects theft, fraud, extortion, and misappropriation charges. A token treated as information cannot easily become the object of theft. Offenders use this gap to argue that no property crime has occurred. Prosecutors shift charges toward computer crimes with lighter penalties. This practice weakens deterrence and produces unequal outcomes for similar conduct. The finding answers the first objective on how criminal law classifies crypto-assets. It shows that classification depends more on judicial choice than on clear legislation. A statutory definition of crypto-assets as property would remove this uncertainty. Such a definition would let courts apply property offences consistently (Kushnirenko, 2023).

Bribery offences committed through digital tokens create serious qualification problems. Traditional bribery laws describe the bribe as money, property, or services. Crypto-assets fit poorly within these terms in several national legal systems. Some courts accept tokens as property benefits, while others demand expert valuation. Valuation becomes difficult be-

cause token prices change sharply within hours. A token worth little today may become extremely valuable within a few weeks. The moment of transfer also creates doubt about when the bribe was completed. A bribe may sit in an unclaimed wallet controlled by a third party. Investigators struggle to link the wallet to the public official. This finding shows that bribery law needs clear rules on digital benefits. Lawmakers should include crypto-assets expressly within the definition of a bribe. Valuation should follow the market price at the moment of transfer. These rules would close a gap that corrupt officials currently exploit (Moiseienko, 2025).

Existing money laundering offences cover crypto-related criminal conduct only partially and unevenly. Most laundering laws focus on funds passing through banks and financial institutions. Crypto laundering often uses mixers, chain-hopping, and decentralized exchanges instead. Each technique breaks the transaction trail that financial investigators normally follow to trace funds. Non-fungible tokens add another layer through fake sales and inflated prices. Courts must prove that the token itself represents proceeds of crime. This proof is hard when transactions pass through many anonymous wallets. Some legal systems fail to treat virtual asset providers as obliged entities. This gap leaves suspicious transactions unreported and criminal funds untraced. The finding answers the second objective on gaps in offence definitions. It shows that laundering law must cover crypto-assets and tokens by express wording. Liability should reach operators of mixing services who knowingly help offenders. Such reform would align criminal law with modern laundering methods (Nazzari, 2025).

Crypto jacking involves secret and unauthorized mining on another person's computing resources. Criminal codes usually lack a separate offence that names this conduct. Prosecutors must choose between unauthorized access, data interference, or theft of electricity. Each option captures only part of the harm caused by attackers. Victims face higher electricity bills, slower devices, and shorter hardware life. Unauthorized access ignores the loss of electricity and hardware life. Theft of electricity ignores the intrusion into a protected information system. Small harm to each victim also leads to weak or symbolic sentences. Large bonnets, in contrast, can affect thousands of devices at the same time. This finding shows that current law fails to reflect the full harm. A specific crypto jacking offence would name the conduct and its typical harms. Penalties should increase where the attack affects many devices or critical systems. This approach would give courts a fair basis for punishment (Nadareishvili, 2022).

Illegal mining farms that steal or misuse electricity raise further qualification problems. Such farms often connect directly to power lines without lawful contracts. They overload local grids and cause blackouts for ordinary households. Some operators bribe local officials to avoid inspections and keep farms running. Some farms operate in regions where mining is banned or restricted. Criminal law usually treats this conduct only as simple theft of electricity from the supplier. This approach ignores damage to energy security and the natural environment. Fines under administrative law are often lower than the profits from mining. Offenders treat these small penalties as a normal business cost. The finding shows that

mining harm needs a broader criminal law response. Lawmakers should create aggravated liability for large-scale illegal mining operations. Confiscation of mining equipment should also become a standard criminal sanction. These measures would make illegal mining unprofitable and protect energy resources (Mauko, 2026).

IV. DISCUSSION & ANALYSES

A. Uncertain Legal Status of Crypto-Assets Weakens Offence Qualification

The uncertain legal status of crypto-assets shapes every later step of criminal qualification. Courts must first decide what a token is before deciding which offence applies. This choice determines whether theft, fraud, or a computer crime becomes the correct charge. The result shows that criminal law still lacks a stable answer to this basic issue. Many criminal codes were drafted before digital tokens became a common means of payment. Their terms such as property, thing, and object assume physical or documentary form. Tokens exist only as entries on a distributed ledger controlled through private keys. This technical nature creates doubt about possession, transfer, and ownership in criminal law. The first research objective asked how existing law classifies crypto-assets in such offences. The answer is that classification currently depends on scattered court practice and expert opinion. Scholars also note that confusing crypto terms makes property offence qualification even harder (Shchehlakov, 2025).

This uncertainty has serious practical effects for courts, prosecutors, and ordinary victims. A victim who loses tokens may find that no property offence fits the loss. Prosecutors may then charge unlawful access, which carries much lighter penalties. Offenders gain a clear advantage from this gap between real harm and the available legal response. Common law courts have started to fill the gap through important civil judgments. The English High Court treated Bit coin as property in *AA v Persons Unknown* in 2019. The New Zealand High Court reached a similar view in *Rescue v CryptoAPI* in 2020. These rulings give criminal courts a useful starting point for future property-based reasoning. Civil recognition does not automatically transfer into criminal statutes and offence definitions. Criminal law demands strict legality, so judges cannot simply extend old terms by analogy. Research on fraudulent crypto transactions confirms that legal uncertainty increases risk for users (Sanz-Bas, 2021).

Recent legislative changes support the view that clear status improves legal certainty. The European Union adopted the Markets in Crypto-Assets Regulation in 2023. It defines crypto-assets and sets uniform rules for service providers. Its full application from December 2024 created a common vocabulary across member states. Russia's Supreme Court recognized virtual assets as possible money laundering objects in 2019. Ukraine adopted a Law on Virtual Assets in 2022 to define their legal nature. Uzbekistan also licenses crypto exchanges and mining through a special state agency. The Law Commission of England and Wales proposed a new category of personal property. These steps show movement toward treating tokens as protected assets. Criminal codes, in contrast, have changed more slowly

than regulatory and civil rules. This delay explains why qualification problems persist despite regulatory progress. European scholars stress that criminal law must now catch up with these regulatory reforms (Troitiño & Hamulák, 2023).

This study also has certain weak points that readers should keep in mind. The analysis relied mainly on doctrinal reading of statutes, judgments, and scholarship. It did not examine large samples of criminal case files from national courts. Access to such files remains restricted in many jurisdictions, especially for cybercrime matters. Interviews with judges and prosecutors could reveal more practical difficulties. The selected legal systems may not reflect practice in every region of the world. Crypto technology changes quickly, so new token types may raise fresh problems. Decentralized finance and stable coins, for example, test definitions in ways not fully covered here. The criminal law focus may understate the role of regulators. Regulatory agencies often detect crypto misconduct long before prosecutors become involved. These points do not weaken the core finding, but they limit its generality. Studies on future financial crime warn that crypto threats will keep evolving rapidly (Trozze, 2022).

The finding agrees with most scholarship that calls for a clear property status. Earlier studies on laundering also found that unclear definitions weaken criminal liability. Some authors, in contrast, argue that tokens should remain digital information only. They fear that property status may extend theft law too far into cyberspace. This view protects legal certainty but leaves many victims without adequate remedies. Some courts already accept tokens as property, while others firmly reject this approach. Other conditions also shape qualification outcomes beyond the text of the law. Judges and investigators often lack technical training on block chain and private keys. Cross-border exchanges make it difficult to trace, freeze, and value stolen tokens. Market volatility complicates the calculation of damage, which affects offence gravity. Political attitudes toward crypto, ranging from bans to promotion, also influence enforcement. Research on criminal liability for laundering shows that weak definitions create serious financial risks (Sharma, 2021).

These results point toward a practical reform path for lawmakers and courts. Legislators should define crypto-assets as property for the purposes of criminal law. Property offences should then name tokens expressly as possible objects of crime. Courts would gain a stable basis for charging theft, fraud, extortion, and robbery. Reform should also cover mining equipment, wallets, and private keys as criminal instruments. Victims would receive protection equal to that given to owners of traditional movable property. Uzbekistan and other reforming states can apply this model within existing codes. Their recent crypto licensing regimes already accept tokens as lawful economic assets. Aligning criminal law with these regimes would remove conflict between legal branches. Training programmers for judges and investigators should accompany any statutory reform. Clear guidance on valuation and proof would further reduce inconsistent court practice. Scholars of technology crime agree that precise offence definitions strengthen deterrence against crypto jacking (Royer, 2023).

B. Crypto-Assets as the Subject of Bribery Remain Poorly Defined

Bribery through crypto-assets exposes a deep gap between old statutes and new payment methods. Most anti-corruption laws were drafted when bribes meant cash, gifts, or services. Officials can now receive value through a wallet address without any physical meeting. This shift makes the bribe invisible to traditional methods of detection and proof. The result shows that courts struggle to fit tokens within the legal subject of bribery. Some judges classify tokens as property, while others call them property rights. A third approach treats them as services, which seems artificial and legally unconvincing. Each choice affects the moment of completion and the calculation of the bribe amount. This answers the first research objective on how crypto-assets enter criminal offence definitions today. Bribery law needs a clear subject before courts can measure guilt and punishment. Crypto bribes also share features of remote crimes, where the parties never physically meet (AllahRakha, 2024).

This gap matters because corruption weakens public trust in every state institution. A corrupt official who accepts tokens may escape liability through technical legal arguments. Defense lawyers often argue that crypto currency is not money, property, or a service. Some courts accept this reasoning and reduce charges to abuse of office. Other courts convict but struggle to assess the value of the bribe. The value matters because many codes grade bribery by the amount received. A token that doubles in price may move a case into a higher category. Courts then face doubt about which date controls the final valuation. Prosecutors must also prove the market rate with expert financial testimony. Victims of corruption, including honest businesses, lose confidence in fair public procurement. Investigators also face problems when wallets sit on servers in foreign countries. Research on block chain crimes shows that establishing jurisdiction over such offenders remains very difficult (Waters, 2023).

Recent practice confirms that crypto bribery is no longer a theoretical concern. A Russian court in 2023 convicted former investigator Marat Tambov for a large bribe in Bit coin. Authorities reportedly seized more than one thousand Bit coin from him, making it one of the largest bribery cases. Russia has required public officials to declare digital currency holdings since 2021. Ukraine added crypto-assets to electronic asset declarations for officials around the same time. The United Nations Convention against Corruption already uses the broad term undue advantage. The United Kingdom Bribery Act similarly refers to any financial or other advantage. These broad terms show how drafting choices can remove doubt about token bribes. National codes with narrow lists of objects remain behind these international standards. Confiscation of seized tokens also requires clear rules on storage, valuation, and sale. New studies show that freezing and confiscating crypto-assets still faces serious legal obstacles (Mauko et al., 2026).

Certain weak points in this study deserve honest attention from readers. Few crypto bribery cases reach courts, so judgments remain limited. Many cases end through plea agreements without detailed written reasoning. This makes it hard to identify stable patterns in judicial practice. Judgments in some countries are not published online or translated into English. Language barriers may also hide useful reasoning from comparative legal research. Media reports may exaggerate amounts or simplify legal issues. The study relied

on published sources and did not access investigative files. Corruption is a hidden crime, so detected cases represent only a small share. Privacy coins and mixers may hide many more bribes than courts ever see. Legal systems outside the selected jurisdictions may apply better solutions. Future research should test these findings through interviews with experienced anti-corruption investigators. Scholars in India similarly report that crypto crimes create serious jurisdictional and enforcement challenges (Watters, 2023).

The finding supports scholarship that calls for an open definition of the bribe. Earlier work on Russian law reached the same view on crypto currency as a bribe. Some authors, in contrast, believe existing terms already cover tokens through interpretation. They argue that property rights include any asset with economic value. This position seems reasonable, yet practice shows that courts apply it inconsistently. Strict legality in criminal law also limits how far judges can stretch old wording. Other conditions shape outcomes beyond the text of bribery statutes. Investigators need block chain analytics tools to link anonymous wallets with specific public officials. Exchanges outside the country may refuse to share customer identity data quickly. Price volatility makes the bribe amount uncertain from transfer to trial. Corrupt officials may also convert tokens into stable coins or cash within hours. Research on crypto currency and money laundering shows how quickly bribe proceeds can be concealed (Adaramola, 2025).

These results suggest a clear reform path for lawmakers and anti-corruption bodies. Bribery provisions should expressly include crypto-assets and other digital rights as possible subjects. The law should fix valuation at the market price on the date of transfer. Courts would then apply consistent amounts when deciding the gravity of offences. Asset declaration rules should require officials to disclose all wallets and private keys. Anti-corruption agencies should receive block chain analytics tools and specialist training. Cooperation with foreign exchanges should become faster through mutual legal assistance agreements. Whistleblower channels could encourage reports of crypto bribes from insiders. Uzbekistan can adopt these steps within its current anti-corruption reform programmed. Similar changes would help other states that are building crypto regulation from scratch. Clear rules would also protect honest officials from unfounded accusations and media pressure. Bribery risks extend to mining permits, where officials may approve harmful projects for illicit rewards (Wiwoho, 2024).

C. Money Laundering Through Crypto-Assets and Non-Fungible Tokens Escapes Traditional Definitions

Money laundering through crypto-assets reveals how fast criminals adapt to new financial tools. Traditional laundering offences assume that dirty funds pass through banks and regulated financial firms. Crypto transfers move directly between wallets without any bank acting as a gatekeeper. Mixers, cross-chain bridges, and decentralized exchanges break the trail between source and destination. Non-fungible tokens add another route through artificial sales of unique digital items. A criminal can buy a token with dirty coins and sell it to a linked account. The inflated price then appears as lawful income from a digital art trade.

The result shows that many codes do not clearly name tokens as laundering objects. This answers the second research objective on gaps within current offence definitions. Courts must prove criminal origin without the paper records that traditional banks normally keep. Research on offences committed through social networks shows that digital crimes escape traditional definitions (Jokić, 2021).

This gap weakens the entire system built to protect financial integrity. Laundered crypto funds can finance drug trafficking, fraud, ransom ware, and terrorism. Each successful laundering scheme rewards the original crime and encourages new offences. Victims of hacks and scams lose any chance of tracing and recovering their assets. Honest exchanges also suffer when criminals use their platforms to clean illicit funds. Regulators may then impose heavy fines that harm innocent customers and investors. Legitimate crypto businesses also find it harder to open bank accounts. Public confidence in digital markets falls when laundering scandals reach the news. States with weak rules may face grey listing by international monitoring bodies. Such listing raises the cost of cross-border payments for ordinary citizens and businesses. Prosecutors need clear offence definitions to turn block chain traces into convictions. A new dataset of centralized and decentralized exchange incidents shows how often platforms become laundering channels (Olushola, 2025).

Recent policy changes show that lawmakers now recognize this danger more seriously. The European Union adopted a new anti-money laundering package in 2024. It created a new European authority to supervise high-risk financial entities from Frankfurt. The Transfer of Funds Regulation now requires crypto providers to share sender and recipient data. This travel rule has applied across the European Union since December 2024. The Financial Action Task Force continues to press states to license and supervise virtual asset providers. In the United States, a jury in 2025 convicted Tornado Cash developer Roman Storm on one charge. Jurors could not agree on the separate money laundering charge against him. This outcome shows how hard it remains to apply laundering law to code developers. The Markets in Crypto-Assets Regulation also excludes most unique non-fungible tokens from its scope. Scholars debate how far European Union competence over crypto-assets should extend externally (Adem, 2026).

Some weak points of this study deserve open discussion. Laundering is a hidden crime, so detected cases show only part of reality. Block chain analytics firms provide much of the public data on illicit flows. Their estimates depend on private methods that outsiders cannot fully check. Different firms often publish different figures for the same year. The study did not test these figures against confidential investigative records. Non-fungible token laundering also has fewer court cases than ordinary crypto laundering. Wash trading in token markets is also hard to separate from genuine speculation. This makes firm conclusions about token-based schemes difficult to reach. Legal systems change rapidly as new rules enter into force each year. Some findings may require updating within a short period of time. Forensic capacity also differs greatly between wealthy and developing countries. Researchers stress that forensic support for investigating virtual asset crimes still needs major improvement (Usatii, 2026).

The finding agrees with studies that call for express mention of crypto-assets in laundering laws. Earlier research on non-fungible tokens reached a similar view on terrorist financing risks. Some authors, in contrast, argue that broad terms like property already cover tokens. They believe courts can reach the same result without any new legislation or amendments. Practice shows mixed outcomes, since judges read these broad terms in different ways. Sentencing also varies widely for similar laundering conduct across national systems. Other conditions shape how laundering cases develop in practice. Privacy coins such as Monero make tracing far harder than Bit coin transfers. Offshore exchanges may ignore requests from foreign investigators for customer records. Decentralized protocols have no company that can freeze suspicious transactions. Rapid price changes also complicate the proof of the laundered amount at trial. Comparative sentencing research shows that criminal law responses to crypto offences remain highly uneven (Tonry, 2026).

These results suggest a clear direction for future laundering reform. Laundering offences should expressly name crypto-assets and non-fungible tokens as possible objects. Liability should extend to mixer operators who knowingly process criminal funds. Courts should accept block chain analytics as admissible proof when experts explain their methods. Non-fungible token marketplaces should fall within customer identification and reporting duties. Investigators need training on bridges, mixers, and wash trading patterns. Exchanges should screen withdrawals to wallets linked with sanctioned mixers. Confiscation rules should allow quick freezing of tokens before offenders move them. Uzbekistan can apply these steps through its licensing system for crypto providers. Regional cooperation within Central Asia would also help trace cross-border laundering flows. Clear rules would protect lawful innovation while closing doors to criminal abuse. Lawmakers must act quickly because offenders keep inventing new methods. Early studies already warned that cyber-criminals rapidly exploit every boom in crypto currency markets (Sigler, 2018).

D. Crypto jacking Lacks a Clear Offence Category

Crypto jacking shows how a new form of harm can fall between existing offences. The attacker does not delete files, steal money, or lock the victim's system. Instead, the attacker secretly borrows the victim's processing power to mine coins for personal profit. Victims rarely notice anything except slower devices and higher electricity bills. The result shows that most criminal codes have no offence that names this conduct directly. Prosecutors must stretch provisions on unauthorized access, data interference, or electricity theft. Each provision protects a different legal interest from the one harmed by crypt jacking. This mismatch answers the second research objective on gaps in current offence definitions. The core harm lies in the unlawful use of computing resources owned by others. Criminal law rarely treats computing capacity as a protected value in its own right. Scholars studying the Japanese Connive litigation ask whether consent less mining should become a separate crime (Benson et al., 2024).

This gap has real consequences for victims, businesses, and public institutions. Even small businesses lose productivity when employee computers run at full capacity. Hospitals,

universities, and government servers have all suffered hidden mining attacks. Each attack consumes energy and shortens the working life of expensive hardware. Cloud accounts can generate huge bills within days when attackers launch mining instances. Courts often view the harm to each single victim as trivial and not serious. This view ignores the combined damage spread across thousands of infected machines. Weak sentences then fail to deter organized groups that operate large bonnets. Victims also struggle to claim compensation without a clear criminal conviction. Insurers may refuse claims when the conduct lacks a recognized legal label. Cyber security teams must spend time and money removing malicious scripts from networks. Global research on crypto currency and crime shows that offenders quickly exploit any weakness in legal controls (Xu et al., 2023).

Recent developments confirm the growing scale of this threat across the world. Japan's Supreme Court in 2022 acquitted a web designer who used the Coin hive mining script. The court held that the script did not qualify as an illegal unauthorized command. This ruling showed how narrow statutory wording can defeat prosecution of hidden mining. In the United States, prosecutors in 2024 charged a man for defrauding cloud providers through crypt jacking. He allegedly consumed millions of dollars in computing resources. The scheme reportedly produced about one million dollars in crypto currency. Security firms reported sharp growth in crypt jacking during 2023. The Council of Europe Convention on Cybercrime covers data and system interference only in general terms. The European Union Directive on attacks against information systems follows a similar general approach. Neither instrument names crypt jacking as a distinct offence. Russian scholars now call for an updated legal mechanism against crypto crimes (Blancaflor et al., 2024).

This study carries some weak points that readers should consider carefully. Official statistics rarely separate crypto jacking from other forms of computer crime. Police records often list such cases under general headings like unauthorized access. This practice hides the true number of reported and prosecuted incidents. Reliable national data on crypto jacking victims remains almost impossible to obtain. The study used published judgments, which cover only a small share of cases. Many attacks are never detected because victims assume their devices are simply ageing. Others are detected but never reported due to embarrassment or low financial loss. Data from security firms may also overstate threats for commercial reasons. Attack methods change quickly as miners move from browsers to cloud and mobile platforms. Some selected legal systems may have unpublished guidance on crypto jacking. Early scholarship on the legal qualification of digital assets already warned that such categories would challenge criminal law (Tiwari et al., 2026).

The finding agrees with studies that call for a specific crypto jacking offence. Hungarian reform offers one example of a country addressing this conduct directly through criminal law. Some scholars, in contrast, argue that general cybercrime provisions are already sufficient. They warn that creating many narrow offences may fragment the criminal code. This argument has merit, yet the Japanese acquittal shows the danger of vague wording. Other conditions also affect how courts treat crypto jacking cases. Attackers often operate from foreign countries, which complicates arrest and extradition. Mined coins usually pass

through privacy tools that hide their final destination. Technical experts are needed to prove which script caused the resource loss. Judges without training may underestimate harm that leaves no visible damage. Low market prices for coins may also reduce the apparent value of losses. Research on asset withdrawal shows that recovering crypto proceeds from criminals requires clear legal procedures (Alekhin, 2025).

These results suggest a practical reform model for lawmakers in many countries. A specific offence should criminalize unauthorized use of another's computing resources for mining. The offence should protect computing capacity as a distinct legal interest. Aggravated penalties should apply to attacks on hospitals, utilities, and government systems. Browser developers and security firms should share threat data with law enforcement agencies. Large bonnets affecting many devices should attract heavier punishment. Courts should calculate harm by combining losses across all affected victims. Confiscation should extend to mined coins, wallets, and infrastructure used in attacks. Website owners should face liability when they embed mining scripts without clear user consent. Uzbekistan can include such provisions in its ongoing cybercrime law reforms. Public awareness campaigns should also teach users to recognize signs of hidden mining. Recent work on block chain and the future of finance stresses that legal certainty supports safe technological growth (AllahRakha, 2024).

E. Illegal Mining Creates Energy and Environmental Harms Outside Criminal Law

Illegal mining shows how a digital activity can produce physical harm. Mining farms run thousands of machines that consume electricity day and night. Many operators avoid paying for this power by connecting directly to distribution lines. Others use subsidized household tariffs meant for ordinary families, not industrial users. Some farms hide inside flats and basements. The result shows that criminal law treats this conduct mainly as simple electricity theft. This approach captures the financial loss to the supplier but ignores wider public harm. Grid failures, fire risks, and environmental damage remain outside the scope of liability. This answers the second research objective on gaps in current offence definitions. Mining links property law, energy law, and environmental law in one activity. Criminal codes still divide these areas into separate chapters with separate protected interests. Scholars observe that the modern legal order struggles to respond to offences involving virtual assets (Mačernytė-Panomariovienė, 2024).

This gap matters because energy is a shared public resource, not a private good alone. Illegal farms overload transformers and cause power cuts for entire neighborhoods. Hospitals, schools, and small businesses then lose electricity during critical hours. Overheated equipment in homes and warehouses has started dangerous fires in several countries. Fossil fuel power used for mining increases carbon emissions and air pollution. Noise from cooling fans disturbs residents near hidden farms. Utility companies pass their losses to honest consumers through higher tariffs. Poor communities often suffer most because they rely on fragile local grids. Rural villages sometimes lose power for days after transformers burn out. Treating such conduct as minor theft sends a weak message to organized operators. A clear

criminal response would better reflect the true social cost of illegal mining. Research from Indonesia shows that illegal crypto mining also deepens climate vulnerability among weaker social groups (Pratiwi, 2026).

Recent events across several regions confirm the seriousness of this threat. Kazakhstan faced repeated blackouts after many miners moved there following China's nationwide 2021 ban. The country then introduced licensing rules and higher energy charges for mining farms. Russia legalized industrial mining in 2024 but banned it in several regions during winter peaks. Malaysia's national utility reported billions of ringgit lost to electricity theft by miners. Kuwait launched a major crackdown on illegal mining homes in 2025 during power shortages. Uzbekistan allows legal mining mainly through solar energy and requires registration with a state agency. Paraguay has also debated much harsher penalties after miners stole power from national lines. These measures show a shift from tolerance toward stricter state control of industrial mining. Most responses, in contrast, rely on administrative fines rather than criminal sanctions. Studies on regulatory effectiveness show that weak penalties rarely deter profitable crypto misconduct (Longa, 2025).

This study has some weak points that deserve careful attention. Illegal farms operate in secret, so their true number remains unknown. Official data often comes from utility companies with commercial interests in high loss figures. Media reports may exaggerate the scale of blackouts. The study did not measure carbon emissions or grid damage through technical data. It relied instead on legal texts, policy documents, and published reports. Satellite and thermal data could offer more objective measures of farm activity. Some countries do not publish court decisions on electricity theft cases online. Mining technology also changes as new machines become more energy efficient. Renewable energy use may reduce environmental harm in certain regions. These points limit how widely the findings apply across different energy systems. Future research should combine legal analysis with energy data and field investigation. Researchers note that data mining methods can strengthen investigation of crypto-related crimes (Venkatasubramanian, 2024).

The finding agrees with scholarship that calls for stronger control over mining activity. Earlier work on crypto mining reform in criminal law reached a similar view on energy harm. Some authors, in contrast, prefer administrative regulation over criminal punishment. They argue that licensing, tariffs, and inspections can solve most problems more efficiently. This view works for legal farms but fails against hidden operators who avoid licensing. Other conditions also influence how states respond to illegal mining. Cheap subsidized electricity attracts miners to countries with weak grid control. Corruption among local officials may protect farms from inspection and disconnection. Sharp Bit coin price rises encourage more illegal mining within weeks. Seasonal demand peaks make grid damage more severe during winter and summer. Political goals also matter, since some states promote mining for foreign revenue. Specialist research on virtual assets shows that criminal qualification of related misconduct remains uneven across jurisdictions (Smith, 2024).

These results suggest a practical model for reform in energy-vulnerable countries. Lawmakers should create a specific offence for large-scale unauthorized mining. The offence

should protect energy security and the environment as distinct legal interests. Aggravated penalties should apply when mining causes blackouts, fires, or damage to public grids. Confiscation of mining machines should become mandatory upon conviction. Profits earned from illegal mining should be traced and confiscated. Landlords who knowingly host illegal farms should share criminal liability. Utilities should share consumption data with police to detect suspicious usage patterns. Smart meters and thermal imaging can help locate hidden farms quickly. Uzbekistan can extend its solar-based mining policy with clear criminal sanctions. Regional cooperation would stop operators from simply moving farms across borders. These steps would protect public resources while allowing lawful mining. Recent engineering research shows that signal processing tools can detect unauthorized mining activity accurately (Popov & Rubtsov, 2024).

F. Implication

This study questions the classic view that criminal law protects only physical property. It shows that crypto-assets, computing capacity, and energy security deserve protection as distinct legal values. The findings support a property-based model for tokens while rejecting the narrow view of tokens as mere information. Clear offence definitions would strengthen deterrence, protect victims, and reduce inconsistent court decisions. Excessive criminalization could discourage lawful innovation and burden honest miners and exchanges. Lawmakers should name crypto-assets in theft, bribery, and laundering provisions and create offences for crypt jacking and illegal mining. Recent steps support this direction, including the European Union Markets in Crypto-Assets Regulation, Russia's 2024 mining law, and Uzbekistan's solar-based mining rules. Japan's Connive acquittal shows the risk of vague wording. Remaining obstacles include cross-border wallets, privacy coins, price volatility, and weak forensic capacity. Courts, prosecutors, victims, energy suppliers, honest businesses, and ordinary citizens would gain from legal certainty. Investigators could use block chain analytics, smart meters, and asset declarations to detect hidden offences. States building new crypto regimes, especially in Central Asia, can adopt this model within existing codes.

V. CONCLUSION

Digital tokens have changed how crimes are committed, hidden, and rewarded. Bribes now travel through wallet addresses, and laundered funds move through mixers and token markets. Hackers secretly borrow computing power, while illegal farms drain electricity from public grids. This study examined why criminal law struggles to classify such conduct correctly. The problem matters because legal uncertainty allows offenders to escape fair punishment. It also matters because victims, honest businesses, and entire communities carry the resulting losses. States across the world now face the same difficulty within their criminal codes. The European Union has adopted the Markets in Crypto-Assets Regulation to bring order to this field. Russia has legalized industrial mining while restricting it in vulnerable regions. Uzbekistan licenses crypto providers and links mining to solar energy.

These reforms show progress, yet criminal law still lags behind regulatory change. Closing this gap is essential for justice in a digital economy.

Three main findings stand out from this study. The first concerns the unclear legal status of tokens within criminal codes. Courts that treat tokens as information cannot apply theft, fraud, or extortion provisions properly. This weakness directly affects bribery cases, where judges disagree on the subject and value of bribes. The second finding concerns laundering, where mixers and non-fungible tokens defeat traditional definitions. Large recent cases, including the Tornado Cash prosecution, show how difficult conviction remains. The third finding concerns crypt jacking and illegal mining, which harm computing resources and energy security. Japan's Connive acquittal reveals how vague wording can defeat prosecution entirely. All three findings share one root, which is the absence of a clear legal status. A single reform model can address them all together. Crypto-assets should become property for criminal purposes, and new offences should cover hidden mining. This approach answers the research question on coherent criminal liability.

These findings offer useful guidance for lawmakers, courts, and enforcement agencies. Legislators can amend property, bribery, and laundering provisions to name crypto-assets expressly. Courts can adopt clear valuation rules based on market prices at the date of transfer. Anti-corruption bodies can require officials to declare all wallets and digital holdings. Energy suppliers and police can share consumption data to locate hidden mining farms. Uzbekistan and other Central Asian states can include these measures in ongoing criminal law reforms. Several questions still need study by scholars and practitioners. Researchers should examine case files and interview prosecutors to test these findings empirically. Decentralized finance, stable coins, and central bank digital currencies deserve separate legal attention. Artificial intelligence may soon automate laundering and mining attacks, creating fresh risks. Comparative work across Asia, Africa, and Latin America would widen knowledge. Criminal law must evolve steadily so that innovation grows without becoming a shield for crime.

VI. BIBLIOGRAPHY

- Brown, A. B., Davis, C. D., & Wilson, E. F. (2024). Contractual frameworks in smart city ecosystems: A systematic review. *Journal of Urban Technology*, 31(2), 145-167. <https://doi.org/10.1080/10630732.2024.123456>
- Adaramola, O. (2025). The dark arts of crypto laundering and the Nigerian financial ecosystem: Examining regulatory perspectives of virtual assets. *Journal of Economic Criminology*. <https://doi.org/10.1016/j.jeconc.2024.100117>
- Adem, M. A. (2026). Reflecting on the EU's exclusive external competence in crypto assets. *European Web Journal of Law*. <https://doi.org/10.14324/111.444.ewlj.2026.01>
- Ageev, V. N. (2025). Cryptocurrency as a subject of bribery: Issues of legal qualification. *Questions of Russian and International Law*, 15(6). <https://doi.org/10.7256/2454-0692.2025.6.77281>
- Al-Balushi, R. H. (2025). Criminal liability for money laundering and terrorist financing through non-fungible tokens. *International Annals of Criminology*. <https://doi.org/10.1017/cr.2025.10114>

- Alekhin, D. E. (2025). Qualification of crimes related to obtaining cryptocurrency (mining). *Courier of Kutafin Moscow State Law University (MSAL)*. <https://doi.org/10.17803/2311-5998.2025.129.5.058-064>
- AllahRakha, N. (2024a). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 16(2).
- AllahRakha, N. (2024b). Cybercrime and the legal and ethical challenges of emerging technologies. *International Journal of Law and Policy*, 2(5), 28–36.
- Antwi, S. (2023). Anti-money laundering measures and financial sector stability in the era of cryptocurrency. *Journal of Financial Crime*. <https://doi.org/10.1108/JFC-03-2023-0045>
- Arnone, G. (2025). The (mis)use of cryptocurrencies by criminal organizations. *European Journal on Criminal Policy and Research*. <https://doi.org/10.1007/s42521-025-00148-1>
- Balaji, A. (2023). Wire fraud on the blockchain: Backdoor prosecutions of insider trading and crypto assets. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4745419>
- Benson, V., Adamyk, B., Chinnaswamy, A., & Adamyk, O. (2024). Harmonising cryptocurrency regulation in Europe: Opportunities for preventing illicit transactions. *European Journal of Law and Economics*, 57(1). <https://doi.org/10.1007/s10657-024-09797-w>
- Blancaflor, E., Dionisio, P. J., Juacalla, D. J., Oraya, A., & Yabut, J. A. (2024). Cryptojacking: A comprehensive review of attack techniques, victims, and effective mitigation strategies. In *Proceedings of the 7th International Conference on Information Systems Security and Privacy*. <https://doi.org/10.1145/3700706.3700713>
- Fernando, Z. J. (2025). Crypto mining as a threat to energy and the environment from the perspective of criminal law reform. *FinTech*, 4(2), 1–11. <https://doi.org/10.3390/FINTECH4020011>
- Gáspár, Z. (2024). The criminalization of cryptojacking in Hungary. *Przegląd Policyjny*, 8(2). <https://doi.org/10.31261/PPK.2024.08.02.01>
- Jokić, D. (2021). A Twitter corpus and lexicon for abusive speech detection: Criminal offenses committed on social networks. *Language Resources and Evaluation*. <https://doi.org/10.1007/s10579-012-9182-3>
- Kushnirenko, S. P. (2023). Cryptocurrencies turnover and forensic analysis of the criminal qualification. *Kriminalistyka*. <https://doi.org/10.33998/2307-5113.2023.1.189>
- Longa, F. A. (2025). Cryptocurrency and money laundering: Regulatory effectiveness in criminal law. *American Journal of Industrial and Business Management*. <https://doi.org/10.6000/2817-2302.2022.01.02>
- Mačernytė-Panomariovienė, I. (2024). The dynamics of modern legal order: Criminal offenses and virtual assets. *Journal of Organizational Behavior*. <https://doi.org/10.1002/job.699>
- Mauko, E., Rubini, S., & Igwe, C. (2026). Evolving trends in cryptomining malware: A systematic literature review. *Crime Science*, 15(1), 14. <https://doi.org/10.1186/s40163-025-00267-5>
- Moiseienko, A. (2025). *Doing business with criminals: Between exclusion and surveillance*. Cambridge University Press. <https://doi.org/10.1017/9781009609845>
- Nadareishvili, I. (2022). Cryptocurrency-related cybercrime types and threats: Focus on cryptojacking. *Law and World*. <https://doi.org/10.32849/2663-5313/2022.1.15>

- Nazzari, M. (2025). How well does the money laundering control system work? *Journal of Law and Economics*. <https://doi.org/10.1086/735665>
- Olushola, A. (2025). The largest unified dataset of CEX and DEX incidents: Criminal liability in crypto exchanges. *Frontiers in Blockchain*. <https://doi.org/10.3389/fbloc.2025.1713637>
- Ordekian, M. (2024). Physical attacks targeting cryptocurrency users. In *Leibniz International Proceedings in Informatics (LIPIcs)*. <https://doi.org/10.4230/LIPIcs.AFT.2024.24>
- Popov, D., & Rubtsov, G. (2024). Digital signal processing in cryptojacking detection and criminal liability. *Digital Signal Processing*. <https://doi.org/10.1016/j.dsp.2024.104594>
- Pratiwi, A. M. (2026). Gender, vulnerability, and power in Indonesia's climate: Criminal law aspects of illegal crypto mining. *Climate and Development*. <https://doi.org/10.1177/27539687221114887>
- Royer, S. (2023). Criminal law and technology in cryptojacking. In *Research handbook on criminal law and technology*. Edward Elgar Publishing. <https://doi.org/10.4337/9781803921327.00020>
- Sanz-Bas, D. (2021). Cryptocurrencies and fraudulent transactions: Risks and perspectives. *Laws*, 10(3), 57. <https://doi.org/10.3390/laws10030057>
- Sharma, A. M. (2021). Cryptocurrency and financial risks: Criminal liability in money laundering. *Scholars Crossing*. <https://doi.org/10.32849/2663-5313/2021.4.22>
- Shchehlakov, I. (2025). Problems of differentiating crypto-terms in the qualification of criminal offenses against property. *Journal of Law and Social Development*. <https://doi.org/10.1007/s11196-023-10083-2>
- Sigler, K. (2018). How cyber-criminals are exploiting the crypto-currency boom: Cryptojacking and criminal law. *Network Security*, 2018(11), 5–8. [https://doi.org/10.1016/S1361-3723\(18\)30086-1](https://doi.org/10.1016/S1361-3723(18)30086-1)
- Smith, D. (2024). *Money laundering, terrorist financing and virtual assets: Criminal qualification*. Springer. <https://doi.org/10.1007/978-3-031-59842-5>
- Tiwari, I. D., Kasturi, Y., & Deebe, S. (2026). Combating digital money laundering: Criminal law perspectives on blockchain-based financial systems. *Economic Sciences*, 22(3), 339–346. <https://doi.org/10.69889/c4e8jt80>
- Tonry, M. (2026). Comparative studies of sentencing: Criminal law responses to crypto offenses. *Crime and Justice*. <https://doi.org/10.1086/739848>
- Troitiño, D. R., & Hamulák, O. (Eds.). (2023). *Europe's criminal law and crypto-assets*. Springer. <https://doi.org/10.1007/978-3-031-27312-4>
- Trozze, A. (2022). Cryptocurrencies and future financial crime. *Technology in Society*. <https://doi.org/10.1016/j.techsoc.2021.101832>
- Usatii, V. (2026). Prospects for improving forensic support in the investigation of crimes involving virtual assets. *Actual Problems of Civil Law and Process*. <https://doi.org/10.32353/acfs.1.2020.09>
- Venkatasubramanian, G. (2024). Artificial intelligence and criminal justice: Data mining in crypto crime investigation. *Statistics and Data Mining*. <https://doi.org/10.1002/sam.11659>
- Watters, C. (2023). When criminals abuse the blockchain: Establishing personal jurisdiction in a decentralised environment. *Laws*, 12(2), 33. <https://doi.org/10.3390/laws12020033>

-
- Wiwoho, J. (2024). Cryptocurrency mining policy to protect the environment. *Cogent Social Sciences*, 10(1). <https://doi.org/10.1080/23311886.2024.2323755>
- Xu, G., Dong, W., Xing, J., Lei, W., Liu, J., Gong, L., Feng, M., Zheng, X., & Liu, S. (2023). Delay-CJ: A novel cryptojacking covert attack method based on delayed strategy and its detection. *Digital Communications and Networks*, 9(5). <https://doi.org/10.1016/j.dcan.2022.04.030>