International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(15s) 2026 pp. 594-603
https://doi.org/10.70917/ijcisim-2026-4224
Article

Securing Digital Borders: Legal Readiness for Cybercrime on Blockchain Investment Fraud by Foreign Nationals

Martanto Dwi Saksomo Hadi[1*], Rudy Agus Gemilang Gultom[2], Ansori[3], Bambang Kustiawan[4]

[1,2,3,4] Department of Defense Strategy, Defense University of the Republic of Indonesia, Bogor Regency, Indonesia

Abstract: This study examines the synergy between blockchain investment fraud and cyberattack schemes by foreign actors that impact a country's economic stability. Using normative research methods with a qualitative approach, this study explores how transnational blockchain-based investment crimes can be "weapons" to disrupt a country's economic stability through attacks on individuals. The research findings indicate a significant gap in law enforcement, as Indonesia has not ratified the Budapest Convention, hampering cross-border evidence collection. Indonesia's cybersecurity policy is also still technocentric, thus failing to mitigate the systemic risks of digital economic aggression through psychological attacks on humans as indirect subjects. As a solution, this study proposes an individual protection framework with an anthropocentric approach that integrates cognitive defense, victim-oriented legal strengthening, and pro-humanitarian technology. Implementing this strategy is crucial for maintaining economic sovereignty and strengthening national cyber defense in the era of decentralization.

Keywords: Anthropocentric Approach, Blockchain, Budapest Convention, Economic Stability, Investment Fraud

1. INTRODUCTION

In this information age, the entire world must face numerous and complex challenges, with cybersecurity being one of the most prominent [1]. Cybercrime can be defined as an extraordinary crime that not only impacts individuals but also extends beyond that to a nation's economy [2]. Cybercrime is also referred to as the fifth domain after land, sea, air, and space in a nation's combat operations [3]. This information transformation is affecting the contemporary battlefield, shifting combat operations to an invisible and intangible fifth domain called cyberspace.

The modern battlefield is no longer limited to direct physical warfare, but has now expanded to encompass a nation's economic infrastructure. Edward Luttwak, in his book "From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce," states that competition between nations has shifted from purely military dominance to economic-based competition (Geo-economics), where access to investment markets and technological mastery have become new "weapons" in the international arena [4]. A country can dominate another country by weakening the economy of a country which is realized through economic instruments such as large-scale fraudulent investments that target certain citizens to trigger serious domestic instability in order to achieve political or strategic goals without the need for open war. This is in line with the opinion of Henry Farrell & Abraham Newman in their research entitled "Weaponized Interdependence: How Global Economic Networks Shape State Coercion" which states that interconnected digital and financial networks can be "weaponized" [5]. Weaponized in this case means it becomes an instrument to attack a country's economy, in this case foreign actors utilize blockchain investments to carry out illegal activities that undermine the economic stability of other countries without having to carry out a physical invasion.

Blockchain systems with decentralized technology that cannot be unilaterally deleted, changed, or manipulated [6], has transformed conventional transactions into using coins such as Bitcoin, Ethereum, USDT, USDC, and others. This dynamic is directly proportional to the risk of crime, such as the offering of new investment fraud schemes [7]. Blockchain investment acts as a dual economic instrument: it can innovate in financial transactions as a new asset with economic value, but it can also be a gateway for new crime models such as online investment fraud, such as

Ponzi schemes, and cyberattacks, which can disrupt national economic stability and potentially drain national economic resources if not reinforced by adequate legal protection [8].

Indonesia's vulnerability to these modern economic weapons is evident in several major cases. The most striking case involves social media artist Indra Kenz who is synonymous with personal branding "Showing off Wealth", this case on November 14, 2022 was sentenced to 10 years in prison and a fine of 5 billion rupiah which if not paid, will be replaced with 10 months in prison because it was proven that he had spread fake news through electronic media and helped consumers who helped in Article 45A paragraph (1), Article 28 paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, as well as committing the Crime of Money Laundering (TPPU) which is regulated in Article 3 of Law Number 8 of 2010 concerning the Prevention and Eradication of the Crime of Money Laundering, this case caused losses to 144 victims totaling 83.3 billion rupiah [9]. Another case that captured public attention was the case of Doni Salmanan, an influencer also known by the nickname. Similar to Indra Kenz, Doni built public trust through a flexing strategy or showing off luxury on social media to lure victims into an investment fraud platform. Doni Salmanan was sentenced to 8 years in prison and a fine of 1 billion rupiah with the provision that if the fine is not paid it will be replaced with 6 months in prison. He was declared legally and convincingly proven guilty of committing the crime of spreading false and misleading news that resulted in consumer losses in electronic transactions, as regulated in Article 45A paragraph (1), Article 28 paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, This case caused losses to 142 victims totaling 24.3 billion rupiah [10].

On a larger scale, Indonesia recorded a case of a transnational Ponzi network in March 2025 that defrauded 90 victims in four major Indonesian cities, namely Jakarta, Surabaya, Medan, and Makassar, which highlighted the seriousness of the loss of 105 billion rupiah [11]. These digital investment crimes are instruments of modern economic warfare. These local actors are merely pawns on a larger chessboard. If the government only takes action against local influencers without disrupting the cyber links to the foreign actors behind them, Indonesia's "Digital Frontline" will remain vulnerable to more destructive attacks. Handling these cases must be elevated from ordinary law enforcement to a national cyber defense strategy. While governments must protect their digital systems and territorial sovereignty, they must also recognize that non-state actors, such as foreigners, including hackers for hire and transnational criminal organizations, are increasingly leveraging decentralized technologies like blockchain to fund illegal activities or undermine national economies [12]. These actors are perfecting malicious techniques that bypass traditional legal jurisdictions, creating a "legal vacuum" that threatens national stability. Therefore, cybersecurity is no longer just a support role for information technology, it is the first line of defense in a holistic national security strategy.

While cybersecurity frameworks for risk management have been widely adopted across the industry [13], their implementation remains highly technocentric, focusing on the technical protection of physical assets rather than private individuals, such as victims of blockchain investment fraud [14], [15], [16]. This raises various issues, such as the government's failure to address how cyberattacks against individuals impact national economic stability through concrete evidence of blockchain-based crimes. Significant gaps also exist in law enforcement when the primary perpetrators are located outside of Indonesia's jurisdiction. This study examines the synergy between blockchain investment fraud and cyberattack schemes in the form of blockchain investment fraud that disrupts the country's economic stability.

2. METHOD

This research is an interdisciplinary research of economics and law. Data collection was conducted through three methods: observation, interviews, documentation, and literature review. Observations were conducted indirectly (content tracking). Researchers searched for keywords on social media platforms (Twitter/X, Facebook, and TikTok) such as "Blockchain Investment Fraud Victims" and "Crypto Investment Fraud" to identify patterns and potential informants.

Next, researchers selected a non-probability sample using a purposive sampling technique. Specific inclusion and exclusion criteria were established to represent the population. Inclusion criteria included informants who experienced fraud in 2025 (blockchain investment), experienced investment losses in the top three highest in the sample population, and were willing to participate. Exclusion criteria included events that occurred outside the 2025 period and were not blockchain-based investment fraud, individuals who were not among the top three losses in the sample population, and informants who did not want to be interviewed.

Interviews were conducted in a relaxed but focused manner via Google Meet to ensure the informants' comfort. Documentation related to the research topic was retained and explained throughout this study.

Interviews with informants were conducted on February 10, 2026, to collect detailed chronological data. The interview instrument was developed based on Professor Atmasasmita's Contemporary Criminal Justice System Theory to construct a complete case scenario. The questions explored the informant's profile, locus & tempus delicti (place and time of the crime), corpus delicti (amount of material/financial loss), modus operandi (chronology and mechanism of the fraud), and additional questions regarding the legal remedies taken by the victim.

The data analysis technique (Legal Economic Analysis) systematically analyzed the collected data using macroeconomic theory John Maynard Keynes [17]. The researchers compared cumulative losses from blockchain investment crimes with Indonesia's Gross Domestic Product (GDP) [18].

$$GDP = C + I + G + (X - M) \quad (1)$$

Formula 1 GDP is a representation of the market value of all final goods and services produced in a region with Consumption (C) reflecting total household or personal expenditure, Investment (I) which refers to business investment and gross fixed capital formation. Government Expenditure (G) which includes government spending on goods and services. Exports (X) and Imports (M) where the difference between the two is called Net Exports (X - M).

This analysis illustrates the correlation between financial losses from cybercrime and the country's economic stability. Furthermore, an analysis was conducted on the legal responsibility of foreign actors based on applicable national and international legal frameworks.

3. RESULTS AND DISCUSSION

3.1. Economic Weapons in Modern Warfare

Since the end of World War II in 1945, conflicts between countries no longer begin with military warfare, but the use of economic instruments as weapons is often done. Attacks on a country's economy have a negative impact on per capita income, poverty, inequality, mortality rates, and human rights. These attacks can be open in the form of economic sanctions that limit the government's access to foreign exchange which has an impact on the country's ability to provide essential public goods and services [19]. The tightened economic sanctions imposed by the United States (US) on the government of Nicolas Maduro in Venezuela in 2017 have put pressure on the country, thus accelerating the transformation of economic policies into authoritarian and neo-patrimonial and authoritarian capitalism [20].

Edward Luttwak said that economic weapons are hidden war tactics to weaken the opponent [4], Economic instruments as tools of coercion in interstate conflicts have evolved from traditional physical blockades to complex digital financial system manipulation in the modern era [21]. In an asymmetric warfare landscape, attacks can shift from conventional military force to financial crimes, weakening a country's economy and creating national instability. Attacks on individuals within a country's population can become a slow but steady incursion that disrupts economic stability. Large-scale investment fraud perpetrated by non-state actors (mercenaries) can be used as a new "weapon" between states to incite instability without physical warfare.

A new chapter is currently underway, the world is being shaken by the arrival of a new financial ecosystem called cryptocurrency based on a decentralized blockchain, automatically without any interference from any party [22]. In line with this, investment instruments have also begun to be marketed, with investment risks directly proportional. Large-scale investment fraud schemes could become one of the most devastating methods of modern economic warfare. Leveraging the narrative of technological advancements with high returns and the use of influencers to "flaunt wealth" can be highly effective in attracting large numbers of investors. Non-state actors and/or foreign syndicates are able to bypass traditional legal jurisdictions, creating a "legal vacuum" that triggers massive capital flight from their victims [23].

This financial tragedy occurred in 2019-2020, known as the "Cryptoqueen" tragedy, where investors invested in the form of Bitcoin, Ethereum, and other crypto assets on a platform called "PlusToken" from China with a return of 10% per month. All investor funds were lost with losses of around 30-45 trillion rupiah [24]. A similar tragedy occurred on the Turkish platform "Thodex", which caused losses of around 42 trillion rupiah to more than 400,000 users in 2021 [25]. These tragedies prove that investment fraud reaches a large value which can have an impact on a country's economy.

Economic weapons are often used by targeting human vulnerabilities and regulatory loopholes, destroying national economic resilience. The annexation of public financial assets through organized blockchain fraud is seen as a continuation of economic imperialist tactics aimed at eroding a nation's sovereignty without firing a single shot. The state's motivation for strengthening individual protection through anthropocentric means is the need to protect citizens from anonymous yet systemic economic aggression. This struggle is not simply a response to ordinary cybercrime, but rather a defense of sovereignty in modern economic warfare.

3.2. Blockchain Investment Online Scams

During a tracking process on social media platforms (Twitter/X, Facebook, and TikTok) using the keywords "Blockchain Investment Fraud Victims" and "Crypto Investment Fraud", researchers discovered that blockchain fraud victims formed an alliance in a WhatsApp group called "BITNEST Indonesia (ID 602)". The group contained a list of victims' names, losses, and residences on the platform called BITNEST.

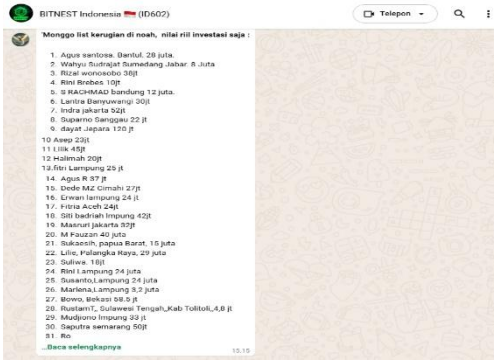

Figure 1. List of Victims in Whatsapp Group

Figure 1 this is evidence that the WhatsApp group "BITNEST Indonesia (ID 602)" contains a list of victims of blockchain investment fraud on the BITNEST platform. Of the total 435 victims, researchers prioritized three individuals who experienced the fraud and suffered the greatest losses.

Table 1. Priority Sample

No	Name	Location	Loss
1	Amirsyah	Bogor	Rp. 342.375.000
2	Saabdullah	Demak	Rp. 180.000.000
3	Anna	Jepara	Rp. 160.875.000

Tabel 1 are informants selected based on the specified inclusion criteria, there are 3 informants out of 435 samples who have listed losses in the WhatsApp group "BITNEST Indonesia (ID 602)". Furthermore, from the interview process with informants, it was found that the informants consisted of three people, namely Amirsyah (32 years old) who lives in Bogor, Saabdullah (37 years old) in Demak, and Anna (27 years old) in Jepara. All three began to realize the fraud at almost the same time, namely around December 12, 2025. Amirsyah stated, "I began to realize that this was a fraud since my funds were not returned as originally agreed upon 24% per month, after December 12, 2025". The same thing was conveyed by Saabdullah who received information that many investment funds did not come in as usual on that date, and Anna who confirmed that on "December 12, 2025 this platform did not pay its users investments anymore".

Each informant had a different way of getting to know the platform. Amirsyah said he was invited by a friend in May 2025 and initially went smoothly with a 24% profit. However, after he invested his entire Rp342,375,000 fund, the funds did not arrive until his contract expired on January 3, 2026. Saabdullah joined in September 2025 at the invitation of a close friend. After initially trying with a small amount and being successful, he invested Rp180,000,000 (approximately $10,714) on November 24, 2025, but the funds were lost despite the platform's previously claimed transparent smart contracts. Meanwhile, Anna became acquainted with the platform in October 2024 through the crypto wallet TokenPocket. Lured by the initial profit, he borrowed Rp 160,875,000 ($9,575) from an online loan to invest on November 20, 2025. He only realized the fraud after checking his crypto wallet and discovering the funds

had not been received. He concluded, “I finally realized this was a blockchain investment scam, promising safe investments with blockchain smart contracts, but in the end, this platform was a scam”.

The material losses suffered by the victims were significant. Amirsyah lost Rp 342,375,000, Saabdullah Rp 180,000,000, and Anna Rp 160,875,000. Regarding legal action, Amirsyah has filed reports online and offline with his group members, although there has been no response. He acknowledged his negligence in not checking with the administrators of the US-registered BisNets.Ltd platform. Saabdullah, on the other hand, chose not to report the case, believing the investment was his own volition and the difficulty of tracking blockchain transactions. Anna also decided not to report it because many other group members had already done so, and she thought this case would be difficult to uncover because the owner of this platform is registered in the United States.

From the 3 informants, there was a total loss of Rp 683,250,000, while the total loss of 435 victims of blockchain investment fraud on the BitNest platform was 10,466,972,000 (10.5 Billion Rupiah).

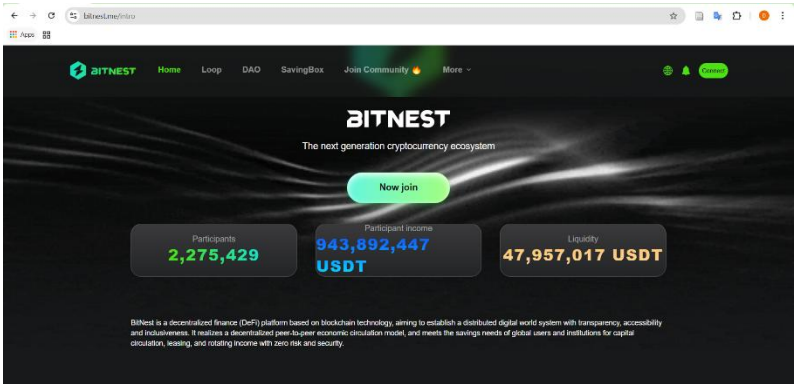

Figure 2. The amount of liquidity on the platform is suspected to be the result of a fake blockchain investment scam

The loss data collected from informants in this study only covers 435 individuals who are members of the instant messaging app group. This figure is still far from the total potential systemic impact, considering that the investment platform currently has 2,275,429 participants. Total liquidity accumulated on the platform reached 47,957,017 USDT. When converted based on the real-time market rate on Saturday, February 21, 2026, when the USDT exchange rate against the Rupiah was in the range of Rp16,858 to Rp16,900, using the midpoint of Rp 16,884, the total liquidity is equivalent to Rp 809,706,275,028. The magnitude of this accumulated funds indicates a very significant economic threat to domestic financial resilience.

3.3. Calculation of State Losses Due to Blockchain Investment Crimes in Comparison with Indonesia’s GDP

The state has a fundamental obligation to protect the human rights of its citizens, where in the principles of criminal law, the state must be able to maintain a balance of protection between the interests of the state, society and individuals [26]. In the context of blockchain-based investment crimes, the losses experienced by individuals cannot be underestimated because the accumulation of these losses has a direct impact on national economic stability. Based on John Maynard Keynes macroeconomic theory approach, through the Gross Domestic Product (GDP) formula.

$$GDP = C + I + G + (X - M) \quad (2)$$

$$GDP = 12.672{,}8\ Trillion\ Rupiah + 6.979{,}6\ Trillion\ Rupiah + 2.143{,}9\ Trillion\ Rupiah + (5.121{,}5\ Trillion\ Rupiah - 4.206{,}3\ Trillion\ Rupiah) \quad (3)$$

$$GDP = 23.821{,}1\ (Trillion\ Rupiah) \quad (4)$$

Throughout 2025, Indonesia’s Consumption (C) is 53.2% of total GDP [27]. Gross Fixed Capital Formation (PMTB) contributes around (I) 29.3% and Government Expenditure (G) 9% [28]. And from the Bank Indonesia (BI) report, the export and import variables (X,M) are 5,121.5 Trillion Rupiah and 4,206.3 Trillion Rupiah [29]. Dengan total PDB Indonesia 23.821,1 (Trillion Rupiah) maka kerugian total 0.0034%.

Although the figure appears small as a percentage of national GDP (0.0034%, or approximately 1 in 30,000 of Indonesia’s 2025 GDP), the Rp 809.7 billion lost from a single platform has a significant impact on the country’s

economic stability. This Rp 809.7 billion loss is equivalent to 0.037% of total Government Expenditure (G), which is projected to reach Rp 2,143.9 trillion in 2025. These funds should have been used to finance the construction of dozens of elementary schools, strengthen military defenses, and build hospitals. From a Household Consumption (C) perspective, this loss represents a direct evaporation of people's purchasing power. Funds that should have circulated in the domestic market and provided a multiplier effect on local economic growth were, in fact, lost without providing any added economic value.

The Rp 809.7 billion loss is evidence of the illicit redistribution of wealth from the Indonesian people to criminals domiciled abroad. This phenomenon confirms that blockchain investment crimes are no longer just small-scale conventional crimes, but rather a form of real "economic leakage". Systematically, if a single illegal platform can raise nearly 1 trillion rupiah, the accumulation of dozens of similar platforms could reach tens of trillions of rupiah. Collectively, this massive financial leakage has the potential to destabilize a country's macroeconomic stability.

3.4. International Legal Review of Blockchain Investment Fraud Crimes

Currently blockchain investment fraud is regulated within the international legal framework of the Budapest Convention on Cybercrime (Budapest Convention), this convention covers criminal acts committed through computer systems [30]. Article 8 on computer fraud requires every party to take legal action according to its national law if someone carries out the action of (a) entering, changing, deleting or hiding computer data, (b) any interference with the functioning of a computer system. With the intention of benefiting themselves or another person [31].

Each country retains full sovereignty over its territory. Failure to ratify the Budapest Convention limits non-member states enforcement powers when perpetrators of crimes are outside the country of a member state. Meanwhile, protecting individuals from blockchain fraud is a state obligation as part of a legal security effort. Non-ratification of this convention presents an obstacle to obtaining digital evidence held on servers in member states due to the lack of standard procedures aligned with Articles 18-21 of the Budapest Convention on cross-border digital evidence collection.

Article 18, concerning production orders, of the Budapest Convention, provides a procedural legal framework for securing digital evidence in cybercrime cases, including blockchain investment fraud. It allows other member states to require crypto exchanges in member states to hand over the identities of users who commit blockchain investment fraud. Article 19 authorizes the seizure and security of technical data, such as private keys or hardware wallets, of perpetrators in member states. Article 20 allows for the tracking of the location of foreign actors through the collection of transaction traffic data. Article 21 authorizes the interception of digital communication content to prove the existence of a crime.

In the case study of blockchain investment fraud in this research, which involves the country of Indonesia, which has not ratified the Budapest Convention [32]. Therefore, its position is very weak to request coercive power to fulfill the contents of the convention that has been agreed upon with other convention members, while the alleged country committing the crime in the case study is a country that has ratified the Budapest Convention.

3.4.1 Law Enforcement of Foreign Actors

Blockchain investment fraud often involves perpetrators from countries other than the victim (foreign actors). Without ratification of international legal conventions such as the Budapest Convention, a country has limited ability to trace perpetrators due to the anonymity of these criminals. Blockchain is transparent yet anonymous, where transactions are conducted openly using random number identifiers, with only the internet service provider and the cryptocurrency exchange where the transaction takes place knowing the user's identity. Law enforcement needs this data to link wallet addresses to the perpetrator's real identity.

Cross-border prosecution of these criminals can be carried out through cooperation agreements or extradition with the perpetrator's country. However, the foreign perpetrator could also be a state actor attempting to weaken the economy of another country. These crimes are difficult to prosecute under international law if committed in Indonesia, as Indonesia has not ratified the Budapest Convention. Therefore, Indonesia can be a safe target for these criminal operations due to the more complex cross-border law enforcement challenges compared to member states of the Budapest Convention.

3.5. The Need for an Investment Framework with an Anthropocentric Approach

Cybersecurity policies addressing the threat of blockchain-based economic aggression require a paradigmatic shift from a rigid technocentric approach to an anthropocentric one that places humans at the center of defense

strategies. Specifically, in cases of blockchain investment fraud, attacks target not only the technical aspects but also the psychology of the victims themselves, who tend to consciously invest in the hope of achieving the returns promised by the investment platform.

In decentralized ecosystems like blockchain investment, the primary vulnerability often lies not in the failure of cryptographic algorithms, but rather in the psychological exploitation of individuals through pig butchering or pyramid schemes, which disrupt economic sovereignty. Therefore, a comprehensive framework is needed that integrates cognitive defense pillars through strategic financial literacy to build the public's cognitive resilience against investment anomalies. This must be reinforced with reactive legal protection aligned with international standards such as the Budapest Convention, to facilitate accelerated asset freezing through cross-agency integration, such as Bappebti and the Indonesian National Police, in responding to the involvement of transnational actors.

Furthermore, the Usable Security pillar requires virtual asset service providers (VASPs) to implement pro-humanity technology through automated early warning systems for high-risk digital wallets, enabling the technology to serve as a secure decision-making tool for ordinary users. Simultaneously, the development of a Recovery Framework that provides psychosocial support is essential to mitigate ongoing sociological impacts and prevent further fraud cycles. Through the implementation of this anthropocentric framework, national resilience can be strengthened by protecting people's purchasing power, increasing public trust in the digital economy, and affirming state sovereignty in minimizing domestic capital leakage due to investment crimes committed by foreign actors in cyberspace.

4. RESEARCH LIMITATIONS

While this study provides insight into the relationship between blockchain investment fraud and a country's economic stability and the barriers to law enforcement by cross-border actors. While this study provides a foundation and insight for the development of national laws ratified from the international legal framework, to protect individual interests that impact national economic stability, this study also has limitations, such as limited analysis because it only assesses the implications for economic stability in Indonesia using a Gross Domestic Product (GDP) approach, with investment fraud losses on a single BitNest platform, the value of which could be more impactful if compared with various investment fraud platforms. It is recommended that future fraud studies utilize various Blockchain-based fraud implementations from various investment fraud platforms and adopt a more holistic and interdisciplinary approach, combining legal analysis with digital forensic audits and behavioral cybereconomic studies to explore the complexities of economic-based cyberwarfare.

5. CONCLUSION

Blockchain investment fraud by foreign actors is not simply a common crime, but a form of economic aggression that cumulatively threatens national economic stability. The unpreparedness of the domestic legal framework, marked by the non-ratification of the Budapest Convention, creates procedural obstacles in pursuing perpetrators and recovering assets across jurisdictions. This is exacerbated by a policy focus that places too much emphasis on technical infrastructure (technocentric), while neglecting the protection of human beings as economic subjects (anthropocentric).

This research confirms that to address this synergy of cyber threats, Indonesia must immediately align its procedural laws with international standards and adopt a comprehensive protection framework. By strengthening digital literacy, regulations that facilitate rapid asset freezing, and providing user-friendly technology, the country can build a more organic defense barrier. Ultimately, protecting individuals from blockchain fraud is an absolute prerequisite for maintaining people's purchasing power, public trust in the digital economy, and the country's financial sovereignty from infiltration by non-state actors in cyberspace.

ACKNOWLEDGMENTS

The author would like to thank all parties who assisted in this research.

FUNDING INFORMATION

The author(s) declare that this research was funded by all authors; no other funding was involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Martanto Dwi Saksomo Hadi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rudy Agus Gemilang Gulto	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓
Ansori	✓	✓	✓	✓	✓		✓	✓			✓	✓	✓	✓
Bambang Kustiawan	✓	✓	✓	✓	✓		✓				✓	✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

All authors declare no conflict of interest with any party.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study. For the benefit of the informants in this study, all names are initialed.

DATA AVAILABILITY

All authors confirm that the data supporting the findings of this study are available within the article.

BIOGRAPHIES OF AUTHORS

Martanto Dwi Saksomo Hadi He is currently pursuing a Doctorate in Defense Science at the Indonesian Defense University (Unhan), focusing his research on cyber defense strategy and national economic protection. He previously completed a Bachelor of Economics and a Master of Science (M.Sc). He is currently actively contributing to strategic thinking in the cybersecurity environment, particularly regarding the National Defense Strategy. He can be reached by email at martanto.dwis@yahoo.co.id.

Rudy Agus Gemilang Gultom He currently serves as the rector of Nurtanio University, Bandung, and a lecturer at the Defense University. He holds a doctorate (S3) with a concentration in defense technology development and is active as a permanent lecturer and promoter in the Doctoral Program (S3) at the Indonesian Defense University (Unhan). He currently serves as an educator in the Department of Defense Strategy, Faculty of Defense Strategy, Unhan. He has published numerous scientific works in leading international and national journals focusing on the integration of advanced technology into military standard operating procedures and protecting digital sovereignty from transnational threats. He is known to be active in formulating cyber risk management frameworks and is a frequent expert resource person at strategic forums on national data security. He can be contacted via email: rudygultom1991@gmail.com.

	**Ansori** He holds a doctorate (S3) in law and a dual master's degree in social sciences and law, strengthening his theoretical foundation in analyzing the phenomenon of transnational crime. He currently serves as a lecturer at the Indonesian Defense University (Unhan), specifically in the Defense Strategy Study Program and is a researcher at the Defense University. His research focuses on the legal aspects of national defense, maritime law enforcement, and the implications of transnational cybercrime for national sovereignty. He actively conducts critical reviews of international legal policies. As a researcher, he has published various strategic studies that serve as references in aligning legal procedures with global regulatory standards. He can be reached by email: navyansori70@gmail.com.
	**Bambang Kustiawan** He holds a doctorate (S3) in management/strategy, and holds a dual bachelor's degree in Economics (S.E) and Social Sciences (S.Sos), complemented by a Master of Management (M.M). He is currently active as a lecturer and researcher at the Indonesian Defense University (Unhan) in the Department of Defense Strategy.

References

1. A. N. Lone, S. Mustajab, and M. Alam, 'A comprehensive study on cybersecurity challenges and opportunities in the IoT world', SECURITY AND PRIVACY, vol. 6, no. 6, p. e318, 2023, doi: 10.1002/spy2.318.
2. S. Caneppele and A. da Silva, 'Cybercrime', in Research Handbook of Comparative Criminal Justice, Edward Elgar Publishing, 2022, pp. 243–260. Accessed: Feb. 18, 2026. [Online]. Available: https://www.elgaronline.com/edcollchap/book/9781839106385/book-part-9781839106385-24.xml
3. M. D. S. Hadi, R. A. G. Gultom, Ansori, and B. Kustiawan, 'Defense Information Systems Architecture for Cyber Threats: A Systematic Review of the Research Literature', Jurnal Penelitian Pendidikan IPA, vol. 11, no. 10, pp. 10–22, Oct. 2025, doi: 10.29303/jppipa.v11i10.12905.
4. M. T. Klare, 'War, Weapons, and Sustainability in the Post-Cold Era', in Building Sustainable Societies: A Blueprint for a Post-industrial World, Routledge, 1996.
5. H. Farrell and A. L. Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', International Security, vol. 44, no. 1, pp. 42–79, Jul. 2019, doi: 10.1162/isec_a_00351.
6. S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, 'Blockchain technology and application: an overview', PeerJ Comput. Sci., vol. 9, p. e1705, Nov. 2023, doi: 10.7717/peerj-cs.1705.
7. Q. Li, M. Ma, T. Shi, and C. Zhu, 'Green investment in a sustainable supply chain: The role of blockchain and fairness', Transportation Research Part E: Logistics and Transportation Review, vol. 167, p. 102908, Nov. 2022, doi: 10.1016/j.tre.2022.102908.
8. U. Agarwal, V. Rishiwal, S. Tanwar, and M. Yadav, 'Blockchain and crypto forensics: Investigating crypto frauds', International Journal of Network Management, vol. 34, no. 2, p. e2255, 2024, doi: 10.1002/nem.2255.
9. B. Agusty and R. Susanti, 'Perlindungan Hukum Korban Binary Option (Studi Kasus Indra Kenz)', UMPurwokerto Law Review, vol. 4, no. 2, pp. 299–308, 2023, doi: 10.30595/umplr.v4i2.16455.
10. D. Setiyawan, M. N. Alhadi, and C. Yassine, 'Asset Restitution Reform to Ensure Legal Protection and Fairness for Investors', Journal of Law and Legal Reform, vol. 5, no. 2, pp. 531–554, Apr. 2024, doi: 10.15294/jllr.vol5i2.1774.
11. R. Anggriawan, 'Countering Transnational Digital Ponzi Schemes in Indonesia: Legal Frameworks, Institutional Challenges, and Reform Pathways', Law and Justice, vol. 10, no. 2, pp. 101–129, Dec. 2025, doi: 10.23917/laj.v10i2.13243.
12. N. Kostyuk and E. Gartzke, 'Fighting in Cyberspace: Internet Access and the Substitutability of Cyber and Military Operations', Journal of Conflict Resolution, vol. 68, no. 1, pp. 80–107, Jan. 2024, doi: 10.1177/00220027231160993.
13. D. M. Rofi'ah, 'NIST Cybersecurity Framework in the Lens of Indonesian Internal Auditors', Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE), vol. 8, no. 2, pp. 3349–3367, Mar. 2025, doi: 10.31538/iijse.v8i2.6027.
14. A. Bhakti, A. Sudirman, R. W. S. Sumadinata, and A. Bainus, 'State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia', Journal of Human Security, vol. 20, no. 1, pp. 109–117, Jul. 2024.

15. N. F. A. Khoiriyah, S. Suwito, and S. Iswati, ‘Analysis of the implementation of defense economic policy in strengthening cyber capacity in Indonesia’, Journal of Economics and Business Letters, vol. 5, no. 6, pp. 37–47, Dec. 2025, doi: 10.55942/jebl.v5i6.1139.
16. R. Rudiyanto and A. Prayitno, ‘Defending the Nation in the Cyber Era: Indonesia’s Response to Non Military Security Threats’, Enrichment: Journal of Multidisciplinary Research and Development, vol. 3, no. 9, pp. 3520–3532, Dec. 2025, doi: 10.55324/enrichment.v3i9.555.
17. D. G. Champernowne, ‘Unemployment, Basic and Monetary: the Classical Analysis and the Keynesian’, in Business Cycle Theory, Part II Volume 7, Routledge, 2005.
18. G. Gündüz, M. Kuzucuoğlu, and Y. Gündüz, ‘Entropic characterization of Gross Domestic Product per capita (GDP) values of countries’, Physica A: Statistical Mechanics and its Applications, vol. 603, p. 127831, Oct. 2022, doi: 10.1016/j.physa.2022.127831.
19. F. Rodríguez, ‘The human consequences of economic sanctions’, Journal of Economic Studies, vol. 51, no. 4, pp. 942–963, Nov. 2023, doi: 10.1108/JES-06-2023-0299.
20. B. Bull and A. Rosales, ‘How Sanctions Led to Authoritarian Capitalism in Venezuela’, Current History, vol. 122, no. 841, pp. 49–55.
21. I. O. Школьник et al., ‘The impact of financial digitalization on ensuring the economic security of a country at war: New measurement vectors’, 2022, Accessed: Feb. 20, 2026. [Online]. Available: https://essuir.sumdu.edu.ua/handle/123456789/89897
22. S. P. Yadav, K. K. Agrawal, B. S. Bhati, F. Al-Turjman, and L. Mostarda, ‘Blockchain-Based Cryptocurrency Regulation: An Overview’, Comput Econ, vol. 59, no. 4, pp. 1659–1675, Apr. 2022, doi: 10.1007/s10614-020-10050-0.
23. ‘Detecting Cryptocurrency Scams in the USA: A Machine Learning-Based Analysis of Scam Patterns and Behaviors’, Journal of Ecohumanism, vol. 4, no. 2, pp. 2091–2111, 2025.
24. J. Scharfman, ‘Ponzi Schemes and Affinity Fraud’, in The Cryptocurrency and Digital Asset Fraud Casebook, Volume III: Exchange Hacks, Deepfakes, Social Media, and Artificial Intelligence Scams, J. Scharfman, Ed., Cham: Springer Nature Switzerland, 2025, pp. 93–116. doi: 10.1007/978-3-031-84108-8_5.
25. J. Botha, V. Luoma-Aho, and L. Leenen, ‘Top Crypto Scams in 2022-2024: Analysing Trends, Tactics, and Regulatory Responses’, in 2025 IST-Africa Conference (IST-Africa), May 2025, pp. 1–9. doi: 10.23919/IST-Africa67297.2025.11060494.
26. P. Vorobey, O. Vorobey, V. Matviichuk, A. Niebytov, and I. Khar, ‘Criminal law principles in the fight against crime’, Revista Amazonia Investiga, vol. 11, no. 49, pp. 156–164, Feb. 2022, doi: 10.34069/AI/2022.49.01.17.
27. Badan Pusat Statistik Indonesia, ‘Ekonomi Indonesia Tahun 2025 Tumbuh 5,11 Persen’, Badan Pusat Statistik, Jakarta, Official Statistics News No. 18/02/Th. XXIX, 5 Februari 2026, 2026. Accessed: Feb. 21, 2026. [Online]. Available: https://www.bps.go.id/id/pressrelease/2026/02/05/2546/ekonomi-indonesia-tahun-2025-tumbuh-5-11-persen.html
28. Kementerian Keuangan Republik Indonesia, ‘APBN Kita Kementerian Keuangan Republik Indonesia’, Kementerian Keuangan Republik Indonesia, Jakarta, Laporan APBN KiTa, 2026. Accessed: Feb. 21, 2026. [Online]. Available: https://www.kemenkeu.go.id/apbnkita
29. Bank Indonesia, ‘Laporan Tinjauan Kebijakan Moneter atau Laporan Bulanan Bank Indonesia’, Bank Indonesia, Jakarta. Accessed: Feb. 21, 2026. [Online]. Available: https://www.bi.go.id/id/publikasi/laporan/Default.aspx
30. F. Spiezia, ‘International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime’, ERA Forum, vol. 23, no. 1, pp. 101–108, May 2022, doi: 10.1007/s12027-022-00707-8.
31. N. M. Apsimet and A. Z. Muratova, ‘On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud’, Bulletin of the Karaganda University “Law Series”, vol. 11730, no. 1, pp. 87–97, Mar. 2025, doi: 10.31489/2025l1/87-97.
32. A. T. Wicaksono and I. F. Yasin, ‘Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection: Reformulasi Hukum Pidana Melalui Omnibus Law Sebagai Solusi Perlindungan Siber Yang Bersifat Sektoral’, Al-Jinayah : Jurnal Hukum Pidana Islam, vol. 10, no. 2, pp. 237–261, Dec. 2024, doi: 10.15642/aj.2024.10.2.237-261.