SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 6097-6108
Open Access. Online & Print

DOI: 10.5281/zenodo.12426634

CYBER-FINANCIAL CRIME LAW ENFORCEMENT CONCEPTS WITH CONVICTION-BASED ASSET FORFEITURE & NON-CONVICTION-BASED ASSET FORFEITURE

Timbo Mangaranap Sirait[1]*, Johan Rosihan[2], Lisno Setiawan[3], Jeremy Nathanael Sirait[4]

[1,2,3,4] Postgraduate Master of Laws, Faculty of Law, Universitas 17 Agustus 1945 Jakarta, Indonesia
Emails: mangaraptimotius@gmail.com[1], Johanrosihan@gmail.com[2], lisnosetiawan@gmail.com[3], siraitjeremylegal@gmail.com[4]

Received: 06/12/2025
Accepted: 15/03/2026

Corresponding Author: Timbo Mangaranap Sirait (mangaraptimotius@gmail.com)

ABSTRACT

Law is inherent in society, including the ever-moving human civilization interactions that shift from real space to cyberspace, which is increasingly sophisticated, and led to the materialization of Cyber-Financial Crime (CFC) which detrimental to the public, prompting the enactment of laws with the best concepts for asset forfeiture of the proceeds globally. This research article was conducted using the normative juridical method with the purpose to analyze the problem, and concluded; First, the law enforcement on CFC in Indonesia still used the concept of Conviction-Based Asset Forfeiture (CBAF), In this context, the assets were only forfeited after the criminal decision final and binding (Inkracht van gewijsde), and due to certain legal obstacles, the judicial decisions insensitive to victims, where judges ruled that all confiscated assets were forfeited to the state, or returned of only a portion; Second, the slow process of returning assets CFC with CBAF concept, prompted the use of Non-Conviction-Based Asset Forfeiture (NCBAF) for the law enforcement as suggested by UNCAC, then legalized through future Asset Forfeiture Law; Third, the best implementation of the recovery of assets between CBAF and NCBAF is still different in various jurisdictions. Hence, some institutions have developed best practice guidelines for prosecuting perpetrators of crimes, and tending to harmonize with NCBAF, although for some cases still use CBAF.

KEYWORDS: Cyber-Financial Crime, Conviction-Based Asset Forfeiture, Law Enforcement, Non-Conviction-Based Asset Forfeiture.

INTRODUCTION

Marcus Tullius Cicero said that where there is a society, there is (system) law [1], so that social interaction was presumed to trigger crimes, eliminated by the creation of laws. The use of adage "*ubi Societas Ibi Ius*," depicts the inherent nature of law in society [2]. At the moment, civilization continues to evolve, with scientific developments influencing the fabric of life, changing the way humans communicate and interact [3], including the investment sector which is usually associated with investing money in real assets or financial assets. Real-world financial interactions have also shifted to electronic systems to cyberspace, because of increasingly sophisticated financial technology [4]. This creates weighty investment opportunities in digital technology both nationally and globally. However, due to rapid advancements, various financial and economic crimes are expected to intensify [5], leading to a rise in Cyber-enabled fraud (CEF). Considering that the exact magnitude and scale have not yet been accurately calculated, its growth has been reported to be weighty and consistent internationally in recent years. The proceeds from these illegal CEFs are often transferred transnationally [6].

In Indonesian jurisdiction, the development of financial technology has created opportunities for the emergence of increasingly sophisticated forms of Cyber-Financial Crime detrimental to the public [7]. Technological advances also enhance criminal practices, as criminals are constantly engaging in new illegal activities [8]. Indonesia Anti-Scam Center (IASC) reported that the number of crime victims continues to increase largely, and in October 2025, the total public losses from various financial fraud methods was roughly IDR 7 trillion [9]. Globally, forms of Cyber-Financial Crime, including Non-Fungible Token (NFT) fraud and sophisticated money laundering, have also been detected, harming the public in 40 countries. These financial activities were stopped by blocking more than 68,000 bank accounts and freezing roughly 400 cryptocurrency wallets, to recover victims' losses [10].

Apart from the reports gotten by IASC, various cases of digital investment fraud under the guise of binary options, which amounted to gambling and Ponzi schemes, were rampant. Many consumers had suffered losses and were victims of fraudulent investments, leading to reports to the police. These binary options are derivative products whose value rely on an underlying asset, such as gold or foreign currency. Each has a predetermined time limit for a single transaction [11]. The most prominent case of illegal investment schemes includes binary option operations performed through platforms namely Binomo, falsely promoted as legitimate Commodity Futures Trading (CFT) instruments. In practice, these operations closely resemble gambling or structured CEF, [12] due to the promotion as legitimate investments. The public is misled into investing funds in the hope of substantial profits, only to fall victim to crime and suffer catastrophic losses.

In Indonesian Jurisdiction, the massive losses caused by the illegal investment scheme, instigated law enforcement to adopt complex efforts to ensnare the perpetrators, specifically affiliates who actively spread false and misleading information through electronic media. Regarding that the case was perpetuated through electronic means in cyberspace, the law enforcement of the investment fraud crime was also *lex specialis* as per the Supreme Court (MA) Cassation Decision Number 2029 K/Pid.Sus/2023. The first charge was in the form of a crime in Article 45 Paragraph (2) in conjunction with Article 27 Paragraph (2). In addition, the third charge was in the form of a crime in Article 45A Paragraph (1) in conjunction with Article 28 Paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 regarding Electronic Information and Transactions ("UU-ITE 2024"). This also included Fraud in Article 378 of the 1946 Criminal Code (*Wetboek van Strafrechts*), and the Criminal Act Law Money Laundering Crime.

The gap between the ideal law (*das sollen*) related to Cyber Law as a special rule (*lex specialis*) and its implementation in addressing digital financial crimes including the support Court Decision for victims as Law in the concrete (*das sein*), was analyzed. This study also monitored the impact of Cyber Law in the 2024 UU-ITE and 1946 Criminal Code (*Wetboek van Straftrechts*) when transformed into the 2023 (Law Number 1 of 2023 concerning the Criminal Code) and 2025 Criminal Procedure Code, intended to be effected simultaneously in January 2026. The global law enforcement policies and institutions related to Cyber-Financial Crime, were critically evaluated with a focus on ensuring the recovery of victims' assets, considering that the flow of criminal funds often included multiple jurisdictions, as well as analized the best law enforcement between CBAF and NCBAF to be applied to confiscating CFC assets, perceived as a limitation and novelty compared to other studies were the perspective of CBAF or civil law only.

Based on the description above, the following problems need to be addressed are with the aim of

finding out: First, how does the concept of law enforcement for asset recovery and protection for victims, resolve the obstacles associated with handling Cyber-Financial Crime in Indonesia?, Second, how does the Implementation of Cyber-Financial Crime law enforcement affect Non-Conviction Based Asset Forfeiture (NCBAF) perceived as an alternative for asset recovery in Indonesia?, Third, how does the Implementation of Cyber-Financial Crime asset recovery with CBAF and NCBAF impact other jurisdictions, including the role of International Institutions?

METHOD

The research was conducted using the Normative Juridical method, through which literature review [13], and a statutory approach were used to examine a series of regulations closely related to the problem under investigation, was adopted. This data included Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 regarding Electronic Information and Transactions ("ITE Law 2024"), Law Number 1 of 1946 concerning Regulations on Criminal Law ("Criminal Code-1946"), Law Number 1 of 2023 concerning Criminal Code ("Criminal Code-2023"), Law Number 8 of 1981 concerning Criminal Procedure Law ("Criminal Procedure Law-1981"), Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes ("Anti-Money Laundering Law"), and the Criminal Procedure Code-2025 ratified on 18 November 2025, Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector, alongside other relevant regulations. Meanwhile, the case approach is carried out by reviewing data the Supreme Court (MA) Cassation Decision Number 2029 K/Pid.Sus/2023 and the role of International institutions related to Cyber-Financial Crime, which is the main focus of this study.

RESULTS AND DISCUSSION

Law Enforcement for Asset Recovery and Victim Protection, as well as Obstacles to Handling Cyber-Financial Crime in Indonesia

The characteristics of Cyber-Financial Crime (CFC), with its highly complex technology and the often deliberate anonymous nature of transactions with the intention of obscuring the fund's origin, were the cause (*causaal verband*) of technical difficulties in identifying and recovering digital assets resulting from crime. This was further worsened by various legal vacuums (*rechtsvacuum*) and regulatory barriers as a basis for law enforcement, including the limitations of related institutions and officials in the financial sector, as stipulated in Article 49 paragraph (5) of PPSK Law. According to the regulation: "Investigations of crimes in the financial services sector may only be conducted by investigators from Financial Services Authority (OJK)." [14].

Legislative constraints further led to a bias in the enforcement of this legal basis. Considering that Indonesian Commodity Futures Trading Regulatory Agency (BAPPEBTI) and the Ministry of Trade, through Article 1 of Ministerial Regulation Number 99 of 2018 concerning the General Policy for the Implementation of Crypto Asset Futures Trading, have recognized crypto as a tradable commodity [15], the 1981 Criminal Procedure Code, Criminal Code-1946, Anti-Money Laundering Law, and the ITE Law-2024 does not yet contain detailed provisions regarding the mechanism for forfeiture or seizure of digital assets [16]. Despite the numerous legal limitations, the principle of legality, stated that in circumstances where there is no violation, punishment could be served only when a criminal provision already exists (*nullum delictum nulla poena sine praevia lege poenali) [17]*. This principle of criminal law must be interpreted strictly in the context of proof, and must not be analogized [18].

The growing number of Internet users has greatly raised the likelihood that electronic data served as the primary evidence in a case [19]. However, the impact of the speed and anonymity of digital financial transactions, alongside material and formal regulatory barriers, in Indonesia, have become real challenges in the law enforcement process, particularly when the procedures are focused on the aspect of CBAF. This entailed fulfilling the validity of digital asset tracking, as well as proving the origin of funds sourced from criminal proceeds.

Regulatory Constraints on the Implementation of Conviction-Based Asset Forfeiture (CBAF) in the Criminal Procedure Code 1981

In many circumstances, the proponent of the electronic evidence, usually the prosecutor, by relying on the doctrine of presumption of reliability (*omnia praesumuntur rite esse acta*) [20]. Prior to the enactment of Electronic Information and Transactions Law, digital evidence was not recognized as valid in Indonesian policy [21]. The fact that Electronic Documents had not yet been recognized as evidence under the Criminal Procedure Code-1981 also served as a weak point at the investigation, prosecution, and trial stages,

specifically in efforts to recover victims' assets under CBAF law enforcement. Technical difficulties comprised procedural law governing blocking and confiscation, carried out by a special institution. Furthermore, the identification of pseudonymous crypto asset ownership with pseudonyms to conceal true identities, and the use of mixers or tumblers in the form of crypto asset mixing services, including mixing funds from various users was aimed to obscure transaction traces. These were realized under the pretext of increasing privacy, all of which were carried out with the intention of obscuring the source of funds, leading to the complication of the link between assets and predicate crimes [22].

The disparity between the speed of digital fund transfers and slow pace of formal legal processes created licit loopholes often exploited by perpetrators [23]. The frequently selected strategy to disguise ownership of complex assets was the use of shell companies in offshore jurisdictions that offered low taxes, confidentiality, or ease of financial record-keeping. This hampered the effectiveness of international cooperation in tracing, confiscating, and recovering losses from victims of financial crimes.

Another obstacle faced by law enforcement with CBAF occurred at the procedural stage of proving the elements of the crime against the perpetrator. In practice, it is difficult to distinguish between losses arising from market risk and structured fraud. This also presented a fundamental obstacle to attesting the existence of malicious intent (*mens rea*) in digital contracts. Proving malicious intent is crucial in determining the perpetrator's criminal liability, particularly in distinguishing between intentional acts (*dolus*) related to committing a crime and mere negligence (*culva*) resulting from business risks. As a result, the confiscation of assets from investment fraud as a predicate crime in conjunction with Money Laundering Crimes becomes extremely crucial. This was because if the element of fraud (predicate crime) cannot be proven convincingly, then the confiscation process cannot be carried out [24], specifically since the assets were often transferred to other countries' jurisdictions. The process made tracking difficult, as well as requires cooperation between countries for the return procedure.

Various additional obstacles related to differences in legal systems and rules of evidence, including the limited authority of national law enforcement to impose judgments in foreign jurisdictions, were regarded as fundamental issues [25]. Furthermore, lack of Mutual Legal Assistance mechanism appropriate to the characteristics of digital assets and the application of double criminality principle made it difficult to receive and enforce Indonesian civil judgments abroad, rendering the asset recovery process ineffective [26]. This was further complicated when assets held in financial centers in certain jurisdictions were protected by the legal system and relevant policies. The procedure complicated the legal process for other countries seeking to return stolen assets and subjected it to the jurisdiction of the nation where the assets were held [27].

Many technical and procedural obstacles related to seizing assets from crime using CBAF, along with emerging regulatory barriers, and the limitations of international legal cooperation frameworks that have not kept pace with the rapidly evolving as well as cross-jurisdictional nature of digital financial crimes, led to difficulties in enforcing the proposed CBAF model. These difficulties are even greater when perpetrators have diplomatic immunity, cannot be located, or in the event of death, which slows down the process of recovering losses for victims.

Handling of Cases with CBAF in Court and Protection of Cyber-Financial Crime Victims

Under the 1981 Criminal Procedure Code, which prioritized CBAF, the status of "crime victims" had received slight attention. Article 46 paragraph (2) of the Criminal Procedure Code-1981 stated that, "when a case has been decided, the confiscated assets shall be returned to the person or persons named in the decision, unless, according to the judge's decision, the assets were impounded for the state," then the rights attached to the assets are transferred to the state [28]. In this criminal procedure law, the policy of returning confiscated assets is up to the judge, and leaves no certainty about the victims' priority. Consequently, judicial decisions are often unfair to victims.

This is evident in the examination of the Tangerang District Court Decision Number 1240/Pid.Sus/2022/PN. For example, on November 14, 2022, a judge's insensitivity to the plight of the victims of Binomo fraudulent investment scheme was clearly evident. The seized assets in the case file, from Exhibit Items 220 to 258, were not returned to the victims rather confiscated for the state. Meanwhile, other portions of Exhibit Items 1 to 219 and 259 to 344 merely complied with the Public Prosecutor's request for criminal prosecution to the South Tangerang District Attorney's Office on October 6, 2022, were not returned to the victims.

The appellate judge at Banten High Court, in its Decision Number 117/PID.SUS/2022/PT.BTN dated January 10, 2023, which examined the facts in

the Appeal, had a different opinion. However, Evidence Items 220 to 258 were finally returned to the victims through the United Indonesian Traders Association (Deed of Establishment Number 21 dated September 26, 2022 before Notary/PPAT Musa Muamarta, S.H.). Regarding Evidence Items 1 to 219 and 259 to 344 in full, the respective status followed the First Instance Decision, and there was no certainty that it would be returned to the victims.

During the examination at the cassation level, through the Supreme Court Decision Number 2029 K/Pid.Sus/2023, the judge stated that Defendant Indra Kenz had been legally and convincingly proven guilty of committing crimes in Electronic Transactions and Money Laundering, punishable under Article 45 Paragraph (2) in conjunction with Article 27 Paragraph (2), Article 45A Paragraph (1) along with Article 28 Paragraph (1) of the ITE Law-2024, including the criminal act of fraud under Article 378 of the Criminal Code-1946. Criminal intent (*mens rea*) was confirmed by the Defendant's deliberate actions in spreading false and misleading news as well as deceitfully raising hopes of instant wealth, as if its members were legally trading. In reality, Binomo had not obtained an official permit from the Commodity Futures Trading Regulatory Agency (BAPPEBTI) in Indonesia.

The restitution of assets for victims of Binomo investment losses, from the first instance judges to the Supreme Court at the cassation level, is still not fully sensitive to the interests of victims. This was because confiscated assets should be returned to the victims in full, as stipulated in the 2005 UN Basic Principles and Guidelines on the Right to Remedy and Reparation. However, this policy had not been fully implemented in the rulings.

Implementation of CBAF in Indonesia After the Enactment of the 2025 Criminal Procedure Code and Protection of CFC Victims

The procedural obstacles to CBAF for the forfeiture of digital assets resulting from Cyber-Financial Crimes (CFC), such as Binomo fraud and Non-Fungible Tokens (NFTs), were virtually eliminated, with the enactment of the new Criminal Procedure Code-2025, ratified on November 18, 2025, in conjunction with the new 2023 Criminal Code-2023. The procedural regulation of the 2025 Criminal Procedure Code expanded the scope of evidence, to complement the Material Criminal Law in the 2024 ITE Law. Article 235 paragraph (1) letter f, reported that it covered "Electronic Evidence," consisting of "Electronic Information," namely "related data that has been processed, with specific meaning in accordance with statutory provisions (Article 1 number 38)." This included "Electronic Documents," such as "Electronic Information created, forwarded, sent, received, stored, viewed, displayed, and heard through a computer or similar system that has a specific meaning or significance in line with statutory provisions (Article 1 number 39)."

Based on Article 112 letters e and f of the 2025 Criminal Procedure Code, investigators may conduct searches of Electronic Information and Documents. These Electronic Evidences contain all forms of data, journals, or systems related to criminal acts.

The 2025 Criminal Procedure Code paid special attention to the blocking of digital assets resulting from cyber-based financial crimes. In urgent situations, blocking that could potentially divert assets or include criminal acts related to information and electronic transactions does not require a judge's approval. Furthermore, Article 144, letters l and v, of the 2025 Criminal Procedure Code provided greater legal certainty for victims, as these individuals have the right to file for restitution through lawsuits and court orders issued after a decision had become legally binding.

Implementation of Cyber-Financial Crime Law Enforcement with "NCBAF" as an Alternative Asset Recovery in Indonesia

The development of digital technology in the Industrial Revolution 4.0 had fundamentally changed the way crimes were committed and the legal response for its enforcement. Over the past two decades, borderless, cross-jurisdictional forms of Cyber-Financial Crime, such as digital investment fraud, theft of NFTs, and crypto-asset money laundering, have challenged national criminal law frameworks that was grounded in territorial and personality principles. Yet, digital asset recovery is inseparable from related issues, international cooperation, and harmonization of national laws.

Following this transformation, the concept of asset recovery has become increasingly strategic, focusing on punishing perpetrators and compensating victims for respective losses, as well as restoring the integrity of the international financial system. In modern legal literature, it is understood as a series of law enforcement actions that include identifying, tracking, freezing, confiscating, managing, and returning assets from criminal activity, both within and outside the home country's jurisdiction [29].

Implementation of NCBAF for Cyber-Financial Crime (CFC) in Indonesia

Indonesia faced serious obstacles due to lack of a non-criminal asset forfeiture (NCB) law [30]. Ideally, the regulations regarding progressive asset forfeiture should go a step further by implementing NCBAF mechanism recommended by UNCAC. This serves as a solution to reclaim digital assets from cyber-financial crime (CFC), which is highly systematic and technologically advanced. UNCAC recommends that countries adopt NCBAF rules to recover misused assets [31]. Through Article 54 paragraph (1) letter c, state parties are required to take the necessary steps associated with the confiscation of assets without having to wait for a criminal decision. Although UNCAC policy was ratified in Law Number 7 of 2006 on the Ratification of the United Nations Convention Against Corruption, 2003, its subsequent implementation had not been comprehensively regulated in related legislation. The implementation was limited to a proposal in the Draft Asset Forfeiture Law (*RUU-Perampasan Aset*), which stated in Article 2, "Asset Forfeiture under this Law was not based on the imposition of penalties on perpetrators of criminal acts." [32].

Following the description above, Nyoman Sarikat Putra Jaya stated the need to ratify the Asset Forfeiture Law, responsible for sanctioning UNCAC confiscation concept. The timeframe was shortened by ensuring the upcoming Asset Forfeiture Law stipulated that the confiscation does not require court proceedings [33]. This mechanism will be enacted as a new procedural law in the future (*Ius Constituendum*) to freeze digital transactions held by asset management institutions suspected of being the proceeds of Cyber-Financial Crimes.

The modern system, through the availability of NCBAF mechanism, allowed for asset confiscation without a criminal conviction. This contradicted the old approach, which relied on CBAF, as well as required lengthy adjudication until the case obtained permanent legal force (*Inkracht van Gewijsde*). The model was based on the principle of in rem (against the object), not *in personam* (against the person/perpetrator), as a result the evidence focused on the origin of the unlawful asset. In the international litigation practice, the basis of a court's jurisdiction (authority to adjudicate), was determined by the distinction generally made between: (1) jurisdiction *in personam*, (2) *in rem*, and (3) *quasi in rem*. Meanwhile, *in rem* is a Latin term meaning "against a thing" or "against something material," referring to a court's jurisdiction to hear cases directed against similar objects [34]. This paradigm shift in the implementation of the recovery process through *in rem* lawsuits is inseparable from the state's efforts to prioritize the confiscation of criminal assets disguised through financial technology (fintech), cryptocurrency, and cross-border electronic payment systems over related proceedings for CBAF.

The Role of the Financial Services Authority in Law Enforcement of CFC Asset Recovery

The issuance of Financial Services Authority Regulation Number 16 of 2023 on the Investigation of Criminal Acts in the Financial Services Sector and the Enforcement of the 2025 Criminal Procedure Code in January 2026, allowed OJK expanded its investigative authority over crimes concerning technological innovation, as well as digital financial and crypto assets. Previously, investigations into cases regarding binary options such as Binomo were conducted by the police prompting OJK to only assist with creating awareness.

Police investigators, due to the advanced equipment used compared to OJK, were quicker and more professional at uncovering the modus operandi of perpetrators of financial crimes [35]. The police were considered to be quick in uncovering perpetrators of cyber-based financial crime and confiscating digital assets. These were processed through court proceedings up to the cassation level, as mandated in the Supreme Court (MA) Decision Number 2029 K/Pid.Sus/2023.

Beyond the legal aspect, digital asset recovery raised an issue of economic justice for victims of online investment crimes in Binomo case, as outlined in the cassation ruling. The victims lost funds, including trust in a legal system that was insensitive to the losses. The 2005 UN Basic Principles and Guidelines on the Right to Remedy and Reparation reported that restitution for victims should be a key element in asset recovery to ensure legal certainty. However, asset recovery law served a dual function, namely a law enforcement instrument and means of restoring substantive justice for victims.

Implementation of Cyber-Financial Crime Asset Recovery with CBAF and NCBAF in Other Jurisdictions and the Role of International Institutions

Recovering assets through information technology in cyberspace entailed more than just confiscation procedures. It also required establishing global legal governance that balanced effective law enforcement, investor protection, and integrity of the international financial system. In this context,

studying the best international practices was crucial as a learning resource for developing countries, including Indonesia.

NCBAF Implementation of Cyber-Financial Crimes in Other Jurisdictions

Several ideas regarding the best way to recover assets from transnational financial fraud outlined the trade-off between respecting national sovereignty and the need for international cooperation. Some countries used NCBAF after completing an investigation, while others adopted it only after criminal proceedings have failed [36].

Countries with common law systems [37], such as the United States and the United Kingdom, tended to be more flexible in allowing NCBAF mechanism. Certain nations with civil law systems, namely France, was more cautious, as confiscation without a criminal conviction could violate the principle of due process. Currently, there is a global trend toward harmonization and acceptance of NCBAF as a legitimate mechanism in addressing transnational crime, specifically following support from UNCAC and Financial Action Task Force (FATF) [38].

In the Dutch legal jurisdiction, whose official system is adopted by Indonesia, Article 10 in conjunction with Article 767 of the Dutch Rv established NCBAF model with as if against a thing (*Quasi in Rem)*. This provision states that if the defendant is outside the Netherlands but has assets in the country, the Dutch court can assume jurisdiction even if the properties are not related to the main issue of the lawsuit. The inclusion of the defendant's fixed assets and movable objects in the legal proceeding, enabled the conferment of the jurisdiction to the Dutch court, commonly known as *Forum Arresti.*

The Role of Stolen Asset Recovery (StAR) in Recovering Assets Proceeding from Cyber-Financial Crimes with NCBAF

Cross-jurisdictional asset recovery in the digital age is closely connected to the role of international organizations, which act as a link between national legal systems. Transnational cyberfinancial crime requires a legal and institutional approach that depends on a single jurisdiction including the principles of mutual legal assistance (MLA) and multi-level coordination among law enforcement, financial institutions, and international agencies [37].

Several global organizations, including the partnership between World Bank and UNODC, established Stolen Asset Recovery **(**StAR) in 2007. It initiated the recovery of stolen assets in cooperation with developing countries and financial centers. StAR was created to support international efforts to end the concealment of criminal proceeds and money laundering, alongside facilitating a more systematic return of stolen assets. The organization previously froze assets related to *the Arab Spring* totaling USD 542.8 million out of USD 1.398 billion, based on legislation passed by Canada, the European Union, and Switzerland, rather than on the request of MLA [39].

StAR program aimed to enhance the countries' ability to identify, freeze, seize, and return transnational criminal assets, describing four strategic pillars, namely strengthening national legal frameworks, building institutional capacity, facilitating international cooperation, and developing best practice guidelines for NCBAF mechanism. Moreover, NCBAF was proposed as an alternative to address the challenges countries faced in prosecuting criminals operating outside the national jurisdiction. The approach was considered legally valid internationally because it was based on the concept of *in rem jurisdiction*, which included the confiscation of objects or assets suspected of being the proceeds of crime without waiting for a criminal sentence against the perpetrator [40].

In the context of cybercrime, StAR Initiative motivated the creation of dedicated Digital Asset Tracing Units (DATUs) in different countries. These units traced digital assets using blockchain analytics, artificial intelligence (AI), and big data forensics. Furthermore, the method allowed law enforcement agencies to follow the movement of crypto assets, often hidden in offshore wallets or transferred through peer-to-peer networks in decentralized financial systems. In 2023, UNODC described this digital innovation as essential for improving the effectiveness of legal systems in tackling Cyber-Financial Crimes.

The Role of FATF with NCBAF in Recovering the Proceeds of Crypto Crime and Non-Fungible Tokens (NFTs)

The use of shell companies in offshore jurisdictions served to conceal complex asset ownership, and this hampered the effectiveness of international cooperation. Accordingly, FATF established by the G7 countries in 1988, officially published the book "Asset Recovery Guidance and Best Practices." The book was the earliest comprehensive guide which specifically addressed strategies, mechanisms, and ideal practices for recovering assets from transnational crime. FATF acts as a global standard-setting body for the

prevention of money laundering (Anti-Money Laundering/AML) and financing of terrorism (Countering the Financing of Terrorism/CFT), including efforts to eliminate fraud and counterfeiting of NFTs, which have recently surged. Indonesia has incorporated various FATF provisions into the national regulation, such as Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering. However, its implementation faced numerous challenges, namely weak coordination among agencies, limited oversight of the non-financial sector, and low compliance with beneficial ownership reporting requirements [41]. This covered competing efforts between OJK and Police, responsible for enforcing laws on virtual assets.

In 2021, FATF published the Forty Recommendations, in which the importance of a legal system that allowed for the seizure and freezing of assets without a criminal conviction (NCBAF), as stipulated in Recommendations 4 and 38, were pinpointed. These recommendations were later expanded to accommodate digital assets through the *Updated Guidance for a Risk-Based Approach to Virtual Assets and Service Providers*. Regarding this guidance, FATF introduced the Travel Rule principle, which mandated Virtual Asset Service Providers (VASPs) to collect and share information about the sender and recipient of cross-border transactions.

FATF recommended the adoption of Risk-Based Approach (RBA) in crypto asset oversight, in 2023. This required countries to deploy law enforcement agencies and officials in high-risk sectors to combat digital money laundering. The guidance was a model adopted by various countries, including the European Union through its 2023 Markets in Crypto-Assets (MiCA) Regulation.

The 2024 FATF report concentrated on the results of the illegal use of NFTs. These were initially introduced on the "Counterparty" platform in 2014. The earliest NFT, dubbed "quantum," was created on the platform, currently valued at millions of dollars [42]. NFT tokens are used on the blockchain to prove ownership of digital assets, namely music, videos, photos, or other art collections, mostly images and moving pictures [43]. Additionally, point 67 of the report stated that NFTs were highly vulnerable to theft and often used for fraud, as well as laundering the proceeds of predicate crimes [44].

The practice of NFT fraud was carried out using manipulative methods in its execution, creating an illusion of authenticity and uniqueness of the fake NFTs. These were then sold under the claim of being unique, and high-value assets. Other methods of counterfeit NFT fraud entailed stealing popular digital artwork or creating fake works that mimic popular styles or content [45].

In 2025, FATF revised its recommendations for asset recovery and international cooperation (2023). This revision was made to improve the understanding of new standards, assist countries in respective implementation, and increase seizures of criminal assets. Asset recovery prioritized the minimization of the desire to profit from crime, curb corruption, enforce laws that provide justice for victims, reinvest funds in society, as well as build the integrity of the financial system and eliminate dirty money from the market.

This organization outlined that asset recovery covered the process of confiscating the proceeds of corruption, as well as an integral part of a national strategy aimed at making crime unprofitable. Moreover, through this guidance, FATF expanded the definition to cover the entire cycle of activities, starting from identification, tracking, freezing, confiscation, management, and return of assets resulting from criminal activity. FATF document was issued as a follow-up to the revisions of the Recommendations & Assessment Methodology of October 2023 and June 2024. Its guidance also outlined the need for several confiscation instruments, such as: 1) *Conviction-Based Confiscation* (CBC), which is centered on a criminal conviction, 2) *Non-Conviction-Based Confiscation* (NCBC), that allows for seizure without a conviction, and 3) *Unexplained Wealth Orders* (UWO) that require asset owners to explain the origin of respective wealth.

Interpol's Role in Recovering Cyber-Financial Crime Proceeds

INTERPOL is the most influential actor in matters of transnational policing with a global reach [46], and founded through an international meeting of law enforcement agencies on September 7, 1923. In Indonesia, the legal basis for NCBs (National Central Bureaus) was regulated by attachment "J" of the Decree of the Chief of Police No. Pol. Kep/53/X/2002 dated October 17, 2002 concerning the Organization and Work Procedures of NCB-Interpol Indonesia Set. The main task was to eradicate crimes that occurred across countries [47], and organized cooperation/coordination through ICPO-Interpol forum. This included crimes whose interactions were carried out through information facilities in cyberspace.

In carrying out its strategic role associated with handling transnational crimes and facilitating international cooperation between police forces, such

as digital asset financial crimes in Cyberspace, Interpol has a global warning system that enables cross-border tracking and arrests without waiting for a complicated formal extradition process. The warning system forms were reported as follows; "Blue Notice" to request information about a person's identity, location, or activities. The "Red Notice" entailed asking a member country to temporarily arrest a wanted suspect or defendant. Additionally, the "Purple Notice" is a request for information about the modus operandi of new digital asset-based financial crimes. The law enforcement model through Interpol is inseparable from the international and regional criminal law framework that regulates the principles of jurisdiction, extradition, mutual legal assistance, and other multilateral cooperation mechanisms [48]. The efforts made by Interpol were carried out through NCB of each country to coordinate between the police work units, ministries and other relevant government agencies [49]. The essence was to resolve or assist in the investigation of digital financial crimes.

Global Rapid Intervention of Payments (I-GRIP) is one of the programs launched by Interpol in 2023. This program is a real-time worldwide coordination system that allows member countries to freeze digital assets obtained from cybercrime before being transferred to another country. Additionally, with support from UNODC Cybercrime Program and Egmont Group, INTERPOL developed 24/7 Secure Communication Channels that enabled the rapid, encrypted exchange of transaction and digital wallet data. The I-24/7 system is an international inter-police communication system that allows members to exchange sensitive and important information securely [50]. This program is groundbreaking due to the ability to overcome bureaucratic obstacles that typically slow down MLA process. Furthermore, the mechanism also inspires the formation of joint investigation teams (JITs) to handle cross-border cases, alongside digital investment-based financial crimes such as Binomo and NFT fraud.

In 2025, Interpol-coordinated criminal law enforcement in 40 countries, under CBAF and NCBAF models, has recovered USD 342 million in criminal proceeds, including USD 97 million in virtual, and physical assets. Meanwhile, Operation HAECHI VI (April - August 2025) which targeted seven types of cyber-based financial crimes, allowed investigators work as a team to detect and stop online fraud (CEF) including money laundering activities, by blocking more than 68,000 bank accounts, and freezing nearly 400 cryptocurrency wallets. This entailed seizing roughly USD 16 million in cryptocurrency wallets suspected of being used for illegal activities.

CONCLUSION

In conclusion, the descriptions and objectives of the study led to the following findings: First, the concept of law enforcement for Cyber-Financial Crime in Indonesia was based on substantive criminal regulation, namely the 2024 ITE Law (*lex specialis*) in conjunction with the 1946 Criminal Code (*lex generalis*) and 1981 Criminal Procedure Code, which were transformed and effected simultaneously in January 2026 to the 2023 Criminal Code and 2025 Criminal Procedure Codes. Its implementation still used CBAF concept, where asset confiscation was only achieved after a criminal verdict against the perpetrator became legally final and binding (*Inkracht van gewijsde*). However, existing legal constraints in the 1981 Criminal Code enabled the inability of "Electronic Documents" to be recognized as "Legal Evidence". This led the difficulty in proving certain cases, including the position of "crime victims" which had not received proper attention in its enforcement. According to Article 46 paragraph (2) of the 1981 Criminal Procedure Code, the decision to return the confiscated results depended on the judge's consideration, and this was evident in the decision of the First Level Judge of Tangerang District Court, who decided that the forfeited asset evidence would not be returned to the victim rather forfeited for the State. Even though the High Court Judge at the Appeal level, reinforced by the Cassation level Judge, stated that it was returned to the victim, not all evidences were returned. The other assets being held had not been prioritized for return to the victim. Therefore, the decision with CBAF was unfair, and not in accordance with the UN Basic Principles and Guidelines on the Right to a Remedy and Reparation in 2005.

Second, Cyber-Financial Crime law enforcement, where due to the slow process and legal uncertainty of returning assets resulting from crime using CBAF asset recovery concept which focuses on punishing the perpetrator. Ideally, its implementation adopted NCBAF concept which was based on the principle *in rem* (against objects), and not *in personam* (against people/perpetrators), further included in the future regulations (*ius constituendum*), following NCBAF asset confiscation concept. This was mandated in Article 54 paragraph (1) letter c UNCAC and ratified by Indonesia through Law No. 7/2006 which "required state parties to take the necessary steps to confiscate assets without the need for criminalization". The policy was legalized through

the Asset Forfeiture Law, which outlined that restitution for crime victims was the main essence as per the UN Basic Principles and Guidelines on the Right to a Remedy and Reparation in 2005.

Third, the implementation of the best approach for recovering assets from Cyber-Financial Crime between CBAF and NCBAF continued to be a tug-of-war between the principle of state sovereignty and the need for global cooperation. Some countries with Common Law systems, such as the United States and the United Kingdom, tended to be flexible in allowing NCBAF mechanism. Meanwhile, certain Civil Law systems accepted NCBAF as stipulated in Article 10 in conjunction with Article 767 of the Dutch Rv with as if against a thing (*Quasi in Rem*). France was more cautious because it considered confiscation without a criminal conviction to be contrary to the principle of due process of law, thereby prioritizing CBAF. Regarding the role of International Institutions that functioned as liaisons between national legal systems for recovering assets from Cyber-Financial Crime, some used CBAF. A trend was observed towards harmonization and acceptance of NCBAF as a legitimate mechanism, specifically following support from StAR, which developed NCBAF best-practice guidelines for prosecuting perpetrators operating outside the national jurisdictions. FATF also issued new standards to increase confiscation through Asset Recovery Guidance and Best Practices in 2025. Interpol, through CBAF and NCBAF, maintained cooperation/coordination through ICPO-Interpol forum as well as launched a real-time global coordination system, namely I-GRIP. This allowed the freezing of digital assets before being transferred to other countries.

REFERENCES

[1] M. A. Syahrin, "THE LEGAL TRADITION IN INDONESIA: FINDING THE MIDDLE WAY (History Aticle)," *Sosiohumaniora: Jurnal Ilmu-ilmu Sosial dan Humaniora*, vol. 24, no. 3, 2022.

[2] A. F. Susanto, H. Septianita, R. Tedjabuana, and M. A. Pratama, *Social Justice Education In Digitalization Era*. Nas Media Pustaka, 2022.

[3] M. S. Prabowo and L. Karimah, "Perlindungan Hukum Bagi Konsumen yang Dirugikan dalam Fintech Lending Transaksi Peminjaman Uang Online Perspektif UU No 8 Tahun 1999," *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, vol. 10, no. 4, pp. 753–768, 2021.

[4] Eny Budi Sri Haryani, "Hukum Investasi Indonesia," Eureka Media Aksara, 2023, p. 13.

[5] Bhavin Shah, "Global Financial and Economic Crime Outlook. Introducing the Secretariat Economic Crime Index 2025," https://secretariat-intl.com/wp-content/uploads/2025/04/ Secretariat-Global-Financial-and- Economic-Crime-Outlook-2025.pdf.

[6] Financial Action Task Force, Interpol, and Egmont Group, "Illicit Financial Flows from Cyber-Enabled Fraud," https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf. coredownload. inline.pdf.

[7] J. H. Napitupulu, M. L. Panggabean, H. Panjaitan, and W. S. Widiarty, "An Integrated Legal Framework for Digital Investment Fraud Prevention in Indonesia," *Journal of Sustainable Development and Regulatory Issues (JSDERI)*, vol. 3, no. 3, pp. 540–567, 2025.

[8] T. M. Sirait and M. H. SH, *Cyber Law dalam Teori dan Perkembangannya (Cyber Crime, Privacy Data, E-Commerce)*. Deepublish, 2024.

[9] Aditya Fajar Indrawan, "Lawan Scam, OJK Gandeng Daerah Perkuat Literasi Keuangan Masyarakat," https://www.hukumonline.com/berita/a/lawan-scam--ojk-gandeng-daerah-perkuat-literasi-keuangan-masyarakat-lt68f4 767 00b 2a0/.

[10] Interpol, "USD 439 million recovered in global financial crime operation," https:// www. interpol .int/en/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation.

[11] F. Ramadani, "Keberadaan Binary Option Ditinjau Dalam Prespektif Hukum Positif Di Indonesia," *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, vol. 13, no. 1, pp. 1–11.

[12] M. Plaikoil, "Law Enforcement In The Case of Binary Option Under The Guise Of Investment and Trading," *Perspektif Hukum*, pp. 92–102, 2024.

[13] S. H. I. Kristiawanto, *Memahami Penelitian Hukum Normatif*. Prenada Media, 2022.

[14] A. S. Ningsih, P. Prananingtyas, A. M. Salwa, F. T. Maharani, and H. P. Wardhani, "Jurisdiction in Financial Crime: A Legal Analysis of the Investigative Authority of Indonesia's Financial Services Authority in Money Laundering Cases," *Jambura Law Review*, vol. 7, no. 2, pp. 468–492, 2025.

[15] H. Widjangkoro, "UPAYA HUKUM TERHADAP INVESTASI CRYPTOCURRENCY DOGECOIN

ILEGAL YANG MERUGIKAN KONSUMEN," *PERSPEKTIF: Kajian Masalah Hukum dan Pembangunan*, vol. 29, no. 2, pp. 72–81, 2024.
[16] D. Hardiago, R. F. Syafrinaldi, M. Musa, and K. Hyeonsoo, "Law and Digitalization: Cryptocurrency as Challenges Towards Indonesia's Criminal Law," *Indonesian Journal of Criminal Law Studies*, vol. 10, no. 1, pp. 297–340, 2025.
[17] D. F. U. Indonesia, "PERCIKAN PEMIKIRAN MAKARA MERAH".
[18] Eddy O.S. Hiariej and Topo Santoso, "Anotasi KUHP Nasional," RajaGrafindo Persada, 2025, p. 5.
[19] S. Chen, R. Rajamanickam, and N. A. Manap, "Legal Framework for Authenticity of Blockchain Electronic Evidence in China: Under a Comparative Law Perspective," *Hasanuddin Law Review*, vol. 10, no. 3, pp. 272–291, 2025.
[20] S. Mason and D. Seng, *Electronic evidence and electronic signatures*, no. 5. University of London, 2021.
[21] M. Lasaka, "Ius constituendum of electronic evidence arrangement in criminal procedure law," *Jurnal Legalitas*, vol. 16, no. 2, pp. 154–166, 2023.
[22] A. Rifai and A. J. Meliala, "Law Enforcement Against Binary Option Trading Affiliators," in *International Conference on Law Studies (INCOLS 2022)*, Atlantis Press, 2022, pp. 148–157.
[23] F. A. T. Force, "Virtual assets red flag indicators of money laundering and terrorist financing," *Consultado en https://www. fatfgafi. org/media/fatf/documents/recomme ndations/Virtual-Assets-Red-Flag-Indicators. pdf*, 2020.
[24] W. Yusmar, S. Somawijaya, and N. S. Putri, "Urgensi Pengesahan Rancangan Undang-Undang Perampasan Aset Tindak Pidana Sebagai Upaya Pemberantasan Tindak Pidana Pencucian Uang Dengan Predicate Crime Tindak Pidana Narkotika," *Jurnal Ilmiah Galuh Justisi*, vol. 9, no. 2, pp. 219–240, 2021.
[25] D. A. Kesuma, "Penerapan mutual legal assistance (mla) dan perjanjian ekstradisi sebagai upaya Indonesia terkait pengembalian aset hasil tindak pidana korupsi," *Lex Lata*, 2021.
[26] Lynda Asiana, Supanto, and Hari Purwadi, "The Implementation of the Double Criminality Principle in the Extradition Treaty of Corruptors Indonesia," *International Journal of Innovation, Creativity and Change* , vol. 11, no. 7, pp. 456–465, 2020.
[27] Mochammad Abizar Yusro and Thufail Rozaan, "Implementasi Perjanjian Mutual Legal Assistance Sebagai Upaya Pengembalian Hasil Kejahatan Di Luar Negeri," *Nagari Law Review* , vol. 4, no. 1, pp. 13–27, 2023.
[28] Luhut Pangaribuan, "Hukum Pidana Khusus: Tindak Pidana Ekonomi, Pencucian Uang, Korupsi dan Kerjasama Internasional Serta Pengembalian Aset," Pustaka Kemang, 2016, p. 594.
[29] T. S. Greenberg, *Stolen asset recovery: a good practices guide for non-conviction based asset forfeiture*. World Bank Publications, 2009.
[30] W. Wulandari, W. Suprayitno, and K. D. Kurniawan, "Asset forfeiture of corruption proceeds using the non-Conviction based Asset Forfeiture Method: A review of Human Rights," *Indonesia Law Reform Journal (ILREJ)*, vol. 3, no. 1, pp. 15–25, 2023.
[31] X. Nugraha, A. M. F. Katherina, W. Agustin, and A. Pamungkas, "Non-Conviction Based Asset Forfeiture Sebagai Formulasi Baru Upaya Stolen Asset Recovery Tindak Pidana Korupsi Indonesia," *Majalah Hukum Nasional*, vol. 49, no. 1, pp. 29–58, 2019.
[32] I. Kamil and F. M. Uce, "Penerapan Non Conviction Based Asset Forfeiture bagi Pelaku Tindak Pidana Korupsi Sebagai Upaya Pengembalian Kerugian Negara," *Simbur Cahaya*, pp. 327–344, 2024.
[33] P. Hikmawati, "Pengembalian Kerugian Keuangan Negara dari Pembayaran Uang Pengganti Tindak Pidana Korupsi, Dapatkah Optimal?(Return of State Financial Losses from The Payment of Substitute Money Corruption Criminal Act, Can It Be Optimal?)," *Negara Hukum: Membangun Hukum untuk Keadilan dan Kesejahteraan*, vol. 10, no. 1, pp. 89–107, 2019.
[34] Syofia M, Tambunan, and et al, "The Concept of In Rem Lawsuits as an Alternative to Confiscation of Assets from Corruption Crime to Recover State Financial Losses in Indonesia," *The IJHSS Journal XIII*, vol. 3, pp. 6–12, 2025.
[35] Marlinda Oktavia Erwanti, "Pengacara Korban Binomo Kritik Hak Penyidikan OJK: Polri Cepat-Profesional," https:// news.detik. com/berita/ d-6501119/ pengacara-korban -binomo- kritik-hak-penyidikan -ojk-polri-cepat profesional.
[36] T. A. Nurdin, "Perbandingan Pengaturan Perampasan Aset Tindak Pidana Korupsi antara Indonesia dengan Amerika Serikat yang Sudah Menerapkan Non-Conviction Based Asset Forfeiture," *Recidive:*

Jurnal Hukum Pidana dan Penanggulangan Kejahatan, vol. 13, no. 2, pp. 134–144, 2024.
[37] T. S. Greenberg, *Stolen asset recovery: a good practices guide for non-conviction based asset forfeiture*. World Bank Publications, 2009.
[38] Financial Action Task Force (FATF), "Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers," https: //www.fatf-gafi.org/ en/publications/ Fatfrecommendations/Guidance-rba-virtual-assets-2021. html.
[39] L. Gray, K. Hansen, P. Recica-Kirkbride, and L. Mills, *Few and Far: the hard facts on stolen asset recovery*. World Bank Publications, 2014.
[40] Y. Husein, *Penjelasan hukum tentang perampasan aset tanpa pemidanaan dalam perkara tindak pidana korupsi*. Pusat Studi Hukum dan Kebijakan Indonesia, 2019.
[41] N. Mouriska and A. Purwati, "PERAN FINANCIAL ACTION TASK FORCE (FATF) DALAM HARMONISASI PENANGGULANGAN PENCUCIAN UANG GLOBAL," *Jurnal Riset Multidisiplin Edukasi*, vol. 2, no. 8, pp. 321–334, 2025.
[42] A. M. Gultom and F. A. Asril, "Key Issues of Non-Fungible Token (NFT): How Transfer of Copyright Should Adapt?," *Perspektif Hukum*, pp. 1–29, 2023.
[43] J. G. Marcelino, N. Kusumawardani, and A. Al Hafiedz, "NFT (Non-Fungible Token) Sebagai Jaminan Kebendaan.," *Notaire*, vol. 6, no. 1, 2023.
[44] F. A. T. Force, "Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers," *Paris, June*, 2022.
[45] I. Matahari, B. A. Saebani, and Y. Sutiana, "Penegakan hukum terhadap pelanggaran pemilihan kepala daerah: Pilkada oleh Badan Pengawas Pemilihan Umum: Bawaslu di Kabupaten Bandung dalam perspektif siyasah dusturiyah," *Ranah Research: Journal of Multidisciplinary Research and Development*, vol. 7, no. 4, pp. 2655–2865, 2025.
[46] G. Calcara, "Balancing international police cooperation: INTERPOL and the undesirable trade-off between rights of individuals and global security," *Liverpool Law Review*, vol. 42, no. 2, pp. 111–142, 2021.
[47] R. J. Manurung, N. Dwiwarno, and J. Setiyono, "Peran Ncb-interpol Indonesia Dalam Rangka Pemberantasan Peredaran Obat Dan Kosmetik Ilegal Dalam Operasi Pangea," *Diponegoro Law Journal*, vol. 5, no. 3, pp. 1–14, 2016.
[48] W. R. Aisya and A. Purwati, "Kolaborasi Interpol dalam Mengatasi Tindak Pidana Ekonomi Lintas Negara: Pendekatan Hukum Pidana Internasional dan Regional," *Jurnal Riset Multidisiplin Edukasi*, vol. 2, no. 8, pp. 565–574, 2025.
[49] M. L. P. Sirait, I. R. Putranti, and H. Susiatiningsih, "Interpol 90th General Assembly and The Securitisation of Better Police Cooperation With National Central Bureau Jakarta," *Global: Jurnal Politik Internasional*, vol. 25, no. 2, pp. 140–163, 2023.
[50] D. A. Kesuma, "Penerapan mutual legal assistance (mla) dan perjanjian ekstradisi sebagai upaya Indonesia terkait pengembalian aset hasil tindak pidana korupsi," *Lex Lata*, 2021.