Law and Justice
Vol. 10, No. 2, 2025, pp. 101-129
e-ISSN: 2549-8282
https://journals2.ums.ac.id/laj/article/view/13243

Countering Transnational Digital Ponzi Schemes in Indonesia: Legal Frameworks, Institutional Challenges, and Reform Pathways

Rizaldy Anggriawan
University of Szeged, Hungary
anggriawan.rizaldy@stud.u-szeged.hu

DOI: 10.23917/laj.v10i2.13243

Submission track:
Revieved:
8 October 2025

Final Revision:
30 December 2025

Available Online:
31 December 2025

Corresponding Author:
Rizaldy Anggriawan
anggriawan.rizaldy@stud.u-szeged.hu

ABSTRAK

Kemajuan pesat dalam transaksi pasar keuangan digital telah mempercepat penyebaran skema Ponzi global, yang menimbulkan ancaman serius bagi negara-negara berkembang seperti Indonesia. Artikel ini meneliti perkembangan skema Ponzi yang melibatkan mata uang kripto, platform perdagangan daring, dan komunikasi terenkripsi yang memungkinkan pelaku menipu investor lintas negara. Tujuan penelitian ini adalah untuk menganalisis hukum dan institusi di Indonesia dalam menghadapi skema Ponzi transnasional. Pendekatan yang digunakan adalah hukum doktrinal, dengan analisis terhadap kasus-kasus penipuan besar yang terjadi antara tahun 2020 hingga 2025, serta tinjauan terbatas terhadap hukum pidana, hukum perbankan, hukum pasar modal, dan undang-undang anti pencucian uang di Indonesia. Meskipun Indonesia memiliki dasar hukum yang memadai untuk menuntut pelaku skema Ponzi, proses hukum menghadapi berbagai kendala, termasuk keterbatasan yurisdiksi, kemampuan forensik digital yang belum optimal, serta tantangan kerja sama lintas negara. Lembaga-lembaga pengatur di Indonesia seperti Otoritas Jasa Keuangan (OJK) dan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) telah melaporkan beberapa langkah awal, seperti pembekuan aset utama kelompok pelaku dan upaya koordinasi investigasi. Namun demikian, masih terlihat adanya kekurangan dalam kesiapan dan kapasitas teknologi. Artikel ini menyimpulkan bahwa reformasi hukum, investasi pada infrastruktur forensik keuangan, kolaborasi internasional yang erat, serta peningkatan kesadaran publik akan sangat penting untuk memperkuat upaya Indonesia dalam memberantas skema Ponzi digital lintas negara dan melindungi investor domestik.

Kata Kunci: *Anti Pencucian Uang, Forensik Digital, Indonesia, Skema Ponzi, Penipuan Transnasional*

ABSTRACT

The dramatic advancement of digitized financial market transactions has enhanced the dissemination of global Ponzi schemes, leading to serious threats to developing nations like Indonesia. This paper investigates the development of Ponzi schemes involving cryptocurrencies, online trading platforms, and encrypted communications in ways that allow them to defraud investors across borders. The aim is to analyze the Indonesia's laws and institutions to deal with the transnational Ponzi schemes. A doctrinal law approach, with case analysis of 'high profile' frauds occurring between 2020 and 2025, combined with a limited capacity to examine the country's criminal law, banking law, capital market law and anti-money laundering laws, leads to the investigation's conclusions. Despite Indonesia having sufficient legal foundations to prosecute Ponzi schemes, any legal proceedings will struggle against many hurdles, including the lack of jurisdiction, digital forensics capabilities, and cooperation across borders. Indonesian regulatory agencies like the Financial Services Authority (OJK) and the Financial Transaction Reports and Analysis Centre (PPATK) reported they have taken some initial steps in freezing the groups major assets and working on coordination of investigations, but it is evident there are degrees of inadequacies of preparedness and technological capacity. The paper finishes with a conclusion that legal reforms, investment in financial forensic infrastructure, critical international collaboration, and raising public awareness will facilitate Indonesia's efforts to disrupt transnational digital Ponzi schemes and protect Indonesian investors.

Keywords: Anti-Money Laundering, Digital Forensics, Indonesia, Ponzi Schemes, Transnational Fraud.

INTRODUCTION

In recent years Ponzi schemes have changed from limited scams into highly advanced frauds, operating over multiple jurisdictions. As schemes become more advanced and complex, they remedy their problems by using digital means - cryptocurrencies, social media, online trading applications, and even artificial intelligence bots to entice investors and hide from regulators. Moving forward, the development of technology has erased the jurisdictional limitations for traditional financial fraud. Criminals are able to victimize an audience abroad while hiding their identity behind layers of encryption, blockchain pseudonymity, and decentralized financial institutions.(Bartoletti et al., 2018) Governments are finding it difficult

to detect, regulate, and potentially prosecute financial crime that does not fit into a paradigmatic form of jurisdiction.

Indonesia, with its youthful and digitally savvy population, has emerged as an active breeding ground for the spread of digital Ponzi schemes. Between 2020 and 2024, Indonesia experienced explosive growth in cryptocurrency investments which occurred on the back of the confluence of inflationary pressures, a speculative frenzy, low financial literacy levels, and a culture of aggressive online marketing. Official data suggests that over 60% of Indonesian crypto account holders are between 18 and 30 years old and cryptocurrency transaction volumes reached IDR 426.69 trillion (roughly EUR 22.47 billion) in just the first nine months of 2024.(Aki, 2024) The rapid uptake of potential investing, while reflective of an important financial innovation and inclusion factor is also reflective of a market that was conducive to actors engaging with fraudulent or Ponzi-like platforms structured as investment opportunities. The issue is illustrated in several case studies. One such case is the March 2025 exposure of a transnational Ponzi network that defrauded at least 90 victims across four major Indonesian cities—Jakarta, Surabaya, Medan, and Makassar—which highlighted both the seriousness of the monetary losses (approximately IDR 105 billion) and the lack of clarity in distinguishing between domestic and foreign actors.(Raidi, 2025)

Within this wider context, the Indonesian experience is an interesting case of the intersection of regulatory capacity, financial innovation, and transnational criminality. Despite the existence of several laws prohibiting fraudulent investment activity, including the Indonesian Criminal Code (KUHP), banking sector laws, capital market laws, and anti-money laundering legislation, law enforcement faced real-time, substantive limitations with jurisdiction, companies' digital environments, and difficulties with identification, limited cyber-forensics capacities of the regulating agencies, and lengthy mutual legal assistance (MLA) requests. On top of this, cryptocurrencies enabled anonymity and end-to-end encryption further inhibited investigative and prosecutorial capacity.(Pratama et al., 2025)

This research aims to assess the advantages and deficiencies with Indonesia's legal frameworks to address cross border Ponzi schemes and, specifically, in the digital era. It looks at how Ponzi schemes have adapted to their digital and transnational infrastructures, if Indonesian legal and institutional responses are adequate to respond to the changing realities. This paper looks at relevant legislation, agencies' roles, enforcement, and case law, in order to evaluate Indonesia's ability to respond to the complexity of cross border financial fraud. The

paper also engages critically with the institutional capacity gaps; to include digital forensics, cybersecurity, and cross border cooperation.

RESEARCH METHOD

The study utilizes a doctrinal legal method, complemented by a qualitative and analytical approach. The use of a doctrinal research methodology is warranted as the focus of the study is centered on understanding and interpreting the body of Indonesian law on cross-border digital Ponzi schemes, including legal texts, regulatory instruments, case law, and institutional practices. By doing so, the study intends to assess the adequacy of the laws and institutional frameworks that are purported to address the complex and evolving nature of Ponzi schemes operating cross-border and within a digital context. The study is considered descriptive in its review of the body of laws, while analytical in assessing their adequacy and enforcement.

The study mainly draws on the study of legal texts and institutional materials as sources of data. Primary sources of information include Indonesian legal texts such as the Criminal Code (KUHP), the Law on the Prevention and Eradication of Money Laundering (Law No. 8 of 2010), the Law on the Financial Services Authority (Law No. 21 of 2011), the Capital Markets Law (Law No. 8 of 1995), the Banking Law (Law No. 10 of 1998), and the Trade Law (Law No. 7 of 2014), as well as applicable implementing regulations and pertinent circulars from institutions. Institutional responses to investment fraud are revealed through policy statements, reports, and press releases and guidance from the Indonesian Financial Services Authority (OJK), the Indonesian Financial Transaction Reports and Analysis Centre (PPATK), the Commodity Futures Trading Regulatory Agency (Bappebti), and Bank Indonesia. Secondary materials for legal commentary, policy analysis and scholarship include academic approaches, scholarly studies, and commentary by legal scholars, practitioners, international reports and databases by organizations such as the United Nations Office on Drugs and Crime (UNODC), the Financial Action Task Force (FATF), and Chainalysis. Findings also include examination of media articles and case records during the 2020 to 2025 range that will be used to consider the relative experiences in enforcement and regulatory recordings.

The research design incorporates a case-based discussion of the identified Ponzi scheme cases within a two to three-year range (2020–2025). Included in the case analysis are the cross-border crypto-investment scheme that was identified in March 2025 across four major cities in Indonesia, the Francius Marganda case involving victims from the diaspora experiencing

victimization in the United States, and additional development of understanding from other identified illegal online investment platforms from the OJK and PPATK. Case studies are analyzed to consider how laws were applied in practice in conjunction with impediments that law enforcement agencies face and institutional factors inhibiting effective responses in cooperation across borders. The case studies also support consideration of an academic understanding of intersections between digital technology, financial regulation, and criminal accountability in the Indonesian context.

RESULTS & DISCUSSION

Evolution of Ponzi Schemes: From Traditional Models to Transnational Digital Fraud

Ponzi schemes continue to pose a growing risk to global financial markets. Ponzi schemes have been around since the earlier part of the twentieth century, but they have changed a lot over the century and accelerated their evolution with advancing technology and globalization. Ponzi schemes prey on investor trust, promising victims high-return investments that they could not reasonably expect to receive anywhere else.(Mugarura, 2017) In the digital age, Ponzi schemes have proliferated and pose a much larger risk to both individuals and the global marketplace. Today, criminals use an array of online platforms, social media, and even cryptocurrencies to continuously engage new investors, all while making it harder for authorities to prosecute. The global focus of digital assets has seen schemes operate internationally. Nowadays, they are almost impossible for law enforcement the track, locate and arrest people involved in these scams. This section will examine the increasing threat of Ponzi schemes. It will continue to define key components of Ponzi schemes, analyze how Ponzi schemes change in the digital age, and provide some accounts of invalid Ponzi schemes that affect different segments of Indonesian society. A thorough understanding of Ponzi schemes and how they are changing, will provide authors with a strong foundation for combating these atrocious financial crimes.

A Ponzi scheme is typically characterized by a fraudulent investment scheme in which returns to previous investors are made using capital contributed by new investors, rather than from profit. Common characteristics typically include guaranteed higher rates of return; little to no transparency; reliance on the constant influx of new capital; and the ability to grow only so long until recruitment slows, or redemptions pick up. Charles Ponzi's scheme in 1920

famously promised 50 % returns in 45 days from the arbitrage of international postal coupons. Although he never possessed more than USD 61 worth of actual postal coupons in his scheme, early investors were paid with contributions from new investors, until investigative journalism by the Boston Post ultimately ended his fraud.(Chen, 2024) Ponzi's name popularized this type of fraud, however various scams such as Sarah Howe's Ladies' Deposit in 1879 predate him.(Weisman, 2020) Later schemes, most notably Bernie Madoff's fraud, swindled investors out of USD 64.8 billion at minimum, using falsified trading records, and collapsed during the financial crisis in 2008.(Abid & Ahmed, 2014)

Aside from financial loss to the individual victims of a Ponzi scheme, perhaps more explosive examples such as the loss of EUR 2 billion in script in Albania in 1996, when the collapse of multiple schemes caused riots in addition to the collapse of a democratically elected government resulting in over 2000 deaths, strongly indicate broader instability risks.(Monroe et al., 2010) Ezubao's example in China, which raised about CNY 50 billion (≈ USD 7.6 billion) from more than 900 000 investors as a P2P online lending Ponzi scheme between 2014-2015, is also illustrative; even after being exposed as a Ponzi scheme, firms such as Ezubao frequently come with a semblance of legitimacy while exploiting regulatory loopholes, collapsing abruptly, eroding trust in financial intermediation, and ultimately resulting in government regulatory responses and pushback to curb consumer fraud.(Liu et al., 2018)

Over the past couple of years, the digital revolution has sped up the advancement of Ponzi schemes. The emergence of cryptocurrencies, ICOs, peer-to-peer platforms, and algorithmic trading bots have provided opportunities for “smart Ponzi” models to take advantage of the credibility established by the technology to attract victims.(Agarwal et al., 2024) The pseudonymous, cross-border nature of crypto-assets only increases the challenges for regulators and forensic investigators. One of the most notable Ponzi schemes related to crypto is BitConnect which launched in 2016. It was promising investors unbelievable yields through a proprietary trading bot, and raised approximately USD 2.4 billion from about 1.5 million victims globally before its collapse in January 2018 after regulators shut it down.(Lensburg, 2024) Likewise, PlusToken attracted about 3 million users, mainly in China and Korea, by promising daily returns and ended up capturing USD 2-3 billion in cryptocurrencies. Repatriation of arrests in 2020 resulted in sentences that ranged from two to eleven years for its masterminds.(Seoul, 2020) While OneCoin was not structured like a Ponzi scheme, but more of a pyramid scheme, it lured global investors into a fake “currency,”

defrauding almost USD 4 billion, prior to arrests of key players; the leader Ruja Ignatova remains at large worldwide.(Scharfman, 2023) Mirror Trading International was a South African crypto platform with a pitch to about 100,000 victims in 140 recipient countries for AI-driven returns, before being declared a pyramid/Ponzi fraud by a South African court in 2023.(Commodity Futures Trading Commission, 2023)

Research by Boshmaf et al (2020) shows that the scale of these digital frauds is enormous. For example, analysis of the MMM scheme (2014–2016) identified daily flows of more than USD 150 million, catastrophic inequality (top earners took the largest share of all total), and massive losses—especially shocking as there was research to show that Indonesian recipients received 12 times the funds that they sent to their Indian counterparts.(Boshmaf et al., 2020) Chainalysis estimates that in Q1 2019 there was more than USD 1.2 billion globally lost to crypto-related fraud, theft and scams, and in total somewhere in the region of USD 1.7 billion in 2018.(Chavez-Dreyfuss, 2019) In 2022, loss of crypto to theft and fraud reached historical highs (more than USD 3 billion).(Lyngaas, 2023) Gupta (2024) reiterates that Ponzi schemes and other frauds especially schemes of the digital era lead to greater market volatility, lowered trust from potential investors, and a move towards greater regulation by government regulators, often resulting in slow innovation.(Gupta, 2024)

Indonesia provides an instructive example of a "double crisis" in the financial sector. Additionally, the country has experienced an explosive growth in cryptocurrency investments. Reports by Indonesian authorities have stated that over 60% of crypto account holders are aged 18-30 and that the total transaction volume in crypto has reached IDR 426.69 trillion (approx. EUR 22.47 billion) in only the first nine months of 2024.(Aprian, 2024) While Indonesian youths' exuberance to invest in crypto is commendable, it cannot mask that there are significant risks involved. The problem of low financial literacy worsens the situation, as desperate people trying to escape inflation seek out "easy money" schemes, and become victims of scams; a situation where online Ponzi and crypto scams, domestically and internationally, have expanded, posing a serious threat to investors and the financial system in Indonesia.(Hidajat, 2018)

In March 2025, Indonesian police identified a cross-border fraud network involving crypto and stock trading that deceived approximately 90 victims across Jakarta, Surabaya, Medan, and Makassar with total loss in the amount of IDR 105 billion (≈ EUR 5.53 million)

where most Indonesian citizens have been victims and perpetrators of international scams.(Arya, 2025) From May 2019–May 2021, Indonesian national Francius Marganda operated a Ponzi scheme based in the U.S. targeting Indonesian–American communities raising over USD 23 million from fake short-term loan schemes promising up to 200–percent returns. He laundered the proceeds into luxury goods and real estate before collapsing in May 2021; in July 2024 he pled guilty and is facing up to 20 years in prison.(U.S. Attorney's Office, 2023) These case examples highlight Indonesia's double burden: while its diaspora is attacked from abroad, e.g. long-standing financial conciseness natives at home are perfongated by scammers.

Legal Frameworks Governing Ponzi Schemes in Indonesia

Ponzi schemes are illegal under Indonesian law, even if this name is not used. It is nevertheless easy to see that Ponzi schemes are a kind of illegal adjunct (fraudulent, deceitful) investment operation promising high investment returns using funds from old investors to pay new investors.(Suwitho et al., 2023) In Indonesia, there is an umbrella for prosecution under *Hukum Pidana* or Criminal Code (*Kitab Undang-Undang Hukum Pidana*, KUHP). Article 378 in the KUHP currently defines any kind of deceitful inducement to money with the following definition: "anyone who, in order to obtain advantage unlawfully for himself or someone else, by deceit or a series of deceits, invokes another person to deliver goods to him or her is threatened with a maximum sentence of four years' imprisonment for fraud." Hence, in practice, any Ponzi-like fundraising is likely to also fall into the category of *penipuan* (fraud).

The revised Indonesian Criminal Code (Law No. 1 of 2023) will take effect in 2026, specifically Article 492 penalizes "Any person who with the intention of gaining an unlawful benefit to himself or another person includes inducing someone to give over an item, shall be punished by a maximum imprisonment of 4 years or fined no more than IDR 500 million (≈ EUR 26,334)." Accordingly, a Ponzi scheme, and other fraudulent or deceptive schemes, will be considered a crime under both the old and new KUHP. There are elements of corporate crime in Indonesia, and thus, if a company's operations represent a Ponzi scheme, corporate officers can be liable under investigations for corporate crime. One legal commentary stated, "If the fraud is by corporation, then the provisions stipulated in Supreme Court Regulation (*Peraturan Mahkamah Agung*, Perma) No. 13 of 2016 also apply" (meaning there is a Supreme Court Regulation on corporate crime that is applicable to investment fraud).

Alongside the KUHP, there are various sector-specific laws that criminalize illegal investment activities. A prime example is laws pertaining to the banking sector. With banking legislation, it is also a crime to raise funds from the public without a legitimate banking license. Under the banking laws, raising funds from the public without a bank license is a crime. For conventional banking, Article 46(1) of Law No. 10 of 1998 (which was amending Law No. 7 of 1992) notes, "Any person who collect the public funds 'savings without the permission of the Head of Bank Indonesia, shall be punished with imprisonment of more than 5 years and not more than 15 years and a fine of more than IDR 10 billion (≈ EUR 526,703) and not more than IDR 20 billion (≈ EUR 1.05 million)." In practice this covers any Ponzi scheme taking "savings" in whatever form without being authorized to do so. Just as the conventional banking law covers illegal collections of "money," Sharia banking law (Law No. 21 of 2008) also prohibits unauthorized collection of investments, and in Article 59, considers it a crime to undertake any Islamic banking or investment business (*dana investasi berdasarkan prinsip syariah*) without Bank Indonesia's license. Punishment was also aligned, offering a sentence between 5–15 years in prison and a fine between IDR 10–200 billion (≈ EUR 0.53 - 10.53 million). These provisions allow the authorities to charge any Ponzi operator that lacked any "legitimate" license as illegal bankers or as illegal fund raisers.

Investment-law provisions also contain provisions on unregistered fundraising. Law No. 8 of 1995 on Capital Markets includes provisions that criminalize any unregistered market activity. Article 103(1) prohibits "Any party that conducts activities in the Capital Market without permission, approval or registration" and subjects any violator to up to 5 years' imprisonment and or a fine of up to IDR 5 billion (≈ EUR 263,853). A Ponzi scheme that poses as an investment fund or securities offering commonly is in violation of this prohibition when it is in the business of collecting money under the guise of an investment fund without a prospectus or approval from OJK (Financial Services Authority).(Setiawan & Ardison, 2021) It is common that the regulatory authorities reference Article 103 to warn of "investment" apps that do not have licenses. Likewise, the consumer-protection and trade laws prohibit pyramid schemes and deceptive marketing. Law No. 7 of 2014 on Trade, for example, contemplates pyramid selling as an unlawful practice: Article 9 forbids "distributing goods or services with a pyramid system", and violators can be imprisoned for up to 10 years and fined up to IDR 10 billion (≈ EUR 526,703) when convicted. This law directly concerns the classic form of multi-

level marketing, but the reasoning could equally apply to Ponzi forms. In practice, regulators have stated that pyramid and Ponzi schemes essentially both "*merugikan*" (harm) the public and they will find them unlawful under the Trade Law. Ministerial regulations (e.g. Ministry of Trade Regulation (*Peraturan Menteri Perdagangan*, Permendag) No. 70 of 2019) direct that pyramid marketing is banned.

Financial regulators also surveil and punish criminal investment activities. The Financial Services Authority (*Otoritas Jasa Keuangan*, OJK) and its Investment Alert Task Force (*Satgas Waspada Investasi*) regularly publish lists of illegal "*investasi bodong*" and have the authority to address criminal violations of banking law, capital markets law, or fintech law. For appreciation the authority of OJK, they have stated that the perpetrators of Ponzi-type schemes usually do not have any approval from OJK, therefore, can be charged based on the capital-market law (Law No. 8 of 1995) or banking law. Additionally, news reports have cited local legal authorities calling upon them to stop an app punting the idea that it is an investment funds, under Article 103 of Law No. 8 of 1995 (prevents unlicensed and unregulated activity in capital markets) to forfeit also has the power to charge under the banking laws (illegal collection of public funds).

In addition to these industry-specific rules, Indonesia's anti-money laundering (AML) regime contains its own mechanisms against transnational fraud. Law No. 8 of 2010 regarding the Prevention and Eradication of Money Laundering which criminalizes the handling of any proceeds derived from any crime. Article 3 of the Law punishes anyone (i) who "places, transfers, diverts or hides or disguises the nature, source, location, disposition, movement, change of ownership, or rights of assets known to be derived from a crime" with up to 20 years in prison and a fine of IDR 10 billion (≈ EUR 526,703); (ii) who "receives or possesses" assets comprised of proceeds from crime with imprisonment of up to 5 years and a fine of up to IDR 1 billion (≈ EUR 52,687). These kinds of provisions relate to the money flows from illicit schemes; in an example, once a Ponzi scheme was established as a criminal scheme, the resultant recovered money could be traced, and confiscated under the Money Laundering Law. Importantly, Article 10 of the 2010 Money Laundering Law captures jurisdiction in an extraterritorial manner: "Any person who is inside or outside the territory of the Republic of Indonesia who participates in an attempt, assists, or conspires to commit the crime of money laundering shall be punished with the same punishment as is provided in Articles 3-5." This

means that Indonesian law can capture laundering acts occurring abroad, in furtherance of a Ponzi scheme, bolstering international cooperation.

Moreover, the new Criminal Code (Law No 1 of 2023) also incorporates elements of universal and passive jurisdiction. Its provisions (Article 8) permit Indonesia to punish its nationals for crimes they commit overseas if those crimes are not already penalized by foreign authorities, as well as to punish those who conspire or assist to commit crimes overseas. The article states "Criminal provisions apply to every Indonesian citizen who commits a crime outside the territory of the Republic of Indonesia." There is nothing new here—the provisions mirror what we see already occurring on the ground under the former KUHP (old penal code). Further, Indonesia has a number of extradition laws and laws on mutual assistance in criminal matters that would allow for some cooperative enforcement. Indonesia has also entered into a number of extradition treaties (such as with some ASEAN countries, among others) and can rely upon mutual legal assistance treaties to obtain evidence or returns of proceeds from criminal activities. (As an example, in the context of a FATF member, Indonesia's laws and agencies including Financial Transaction Reports and Analysis Center (*Pusat Pelaporan dan Analisis Transaksi Keuangan*, PPATK), which is the Indonesian Financial Intelligence Unit (FIU)—participate in cross-border AML investigations with a number of other countries). Though there are not mechanisms specific to Ponzi cases, the international cooperation outlined above indicates that Indonesia's legal framework is intended to capture transnational economic crime in a broad sense.

Institutional Roles and Enforcement Mechanisms

Indonesia has seen an alarming spike in cross-border investment frauds in recent years. A Ponzi scheme, an illegal investment scheme that pays earlier investors off with money from new investors, is inherently transnational when part of the online ecosystem. Indonesia has deployed a tiered institutional structure of regulators, financial intelligence, law enforcement actors, and coordinating task forces to counter this type of fraud. The Financial Services Authority (OJK), the Financial Transaction Reports and Analysis Center (PPATK), the commodity futures regulator (*Badan Pengawas Perdagangan Berjangka Komoditi*, Bappebti), the central bank (Bank Indonesia), the Ministry of Trade, as well as communications authorities, police/prosecutors, have legal mandates pursuant to established laws. Each of these authorities

reviews a web of regulations and laws that treat Ponzi operations as at least one if not several criminal violations; they coordinate their actions nationally and internationally to detect and disrupt Ponzi schemes. This part reviews each institution's responsibilities, legal provisions, and tangible responses to removing transnational Ponzi schemes from Indonesia.

The Financial Services Authority (OJK) is the lead regulator for banks, securities, and non-bank financial services. Law No. 21 of 2011 also explicitly defines OJK as an "independent", integrated regulator for "supervision and regulation" of the financial services sector and consumer and public interest activities. In practice, OJK appears to monitor proposed investment offerings for licenses and educating the public about fraud. OJK, for example, has warned since 2015 that unsolicited "investment" messages through SMS, email or websites which showed normal Ponzi characteristics; such as: promised extraordinarily high guaranteed returns, a global recruitment network, no real underlining product, no license from regulators.(Otoritas Jasa Keuangan, 2015) OJK continued to lead the multi-agency *Satgas Waspada Investasi* (Investment Alert Task Force). The Investment Alert Task Force identified in mid-2022 (July 2022 press release) 10 non-approved investment offerings in "money games" (Ponzi schemes) and has now compelled and forced two players to stop operations and return money to investors. In that press release OJK publicly named *PT Enel Kekuatan Hijau* and demanded they return the money to the victims of their Ponzi scheme as one of the illegal players.(Otoritas Jasa Keuangan, 2022)

OJK has recently enhanced its defenses against online scams. In late 2024 it launched the Indonesia Anti-Scam Centre (IASC), which is a center for reporting and coordination of digital financial fraud. OJK officials said that by May 2025, the IASC processed over 128.000 reports of scams and assisted in freezing IDR 2.6 trillion (≈ EUR 137 million) in losses.(Isaac, 2025) OJK is also strengthening regulations by its new Consumer Protection Rule (*Peraturan Otoritas Jasa Keuangan*, POJK No. 22 of 2023) includes rights to data privacy and transparency and explicitly allows OJK to provide legal aid to consumers who have been scammed. In terms of enforcement, OJK worked with banks to quickly block suspicious accounts. A 2015 OJK press release recalled that “several banks have been able to block the perpetrators after the immediate inter-bank cooperation by blocking the accounts of both the sender and receiver,” and urged all banks to act quickly on detected fraud to protect customers' funds.(Otoritas Jasa Keuangan, 2015) In order to combat transnational fraud, OJK draws upon access to the global

financial landscape; for example, it has worked with foreign regulators through its membership in international organizations (such as International Organization of Securities Commissions (IOSCO) and regionally), as well as foreign assistance through their investigations of Indonesia-based schemes.(Otoritas Jasa Keuangan, 2016) OJK's legal mandate (Law No. 21 of 2011), along with their more recently enacted regulations, has made OJK a front line organization to identify illegal investment offerings and provide protections for retail investors. OJK's efforts to educate and warn the public, along with SWI task force efforts, are instrumental in minimizing the use of transnational Ponzi schemes to Ponzi scam Indonesians.

In addition to the OJK, Indonesia has the Financial Transaction Reports and Analysis Center (PPATK), which is Indonesia's anti-money laundering agency, or Financial Intelligence Unit. Founded under the first anti-money laundering law in 2002, PPATK was expressly designed to strengthen Indonesia's position in coordinated efforts to combat transnational organized crime globally. As set out in Law No. 8 of 2010 (amending the original 2002 law), PPATK is tasked with preventing and eradicating money laundering, which includes proceeds from predicate offences such as fraud. Article 44 of Law No. 8 of 2010 empowers PPATK specifically as follows: "The PPATK may request financial service providers to temporarily suspend all or part of any transaction known or suspected to be the proceeds of crime." Article 44 also gives PPATK the ability to share intelligence with other investigative authorities, whether domestic or foreign. In practice, PPATK uses this authority robustly against Ponzi schemes. For example, in April 2022 PPATK revealed that it had frozen 345 bank accounts related to illegal investment funds (approximately IDR 588 billion, ≈ EUR 30.88 million). Investigators found that many Ponzi fund flows were camouflaged by cryptocurrency and many mutiple bank transactions in order to disguise these money trails. Because of PPATK's analysis, those accounts were blocked very quickly. Ivan Yustiavandana, PPATK's head, reported that as of early 2022 PPATK had also blocked 275 suspicious transactions involving IDR 502 billion (≈ EUR 26.37 million) related to illegal investments. These are tangible examples of PPATK's utilization of the freezing powers under Article 44 to dismantle Ponzi networks.(Hutasoit, 2022)

Part of PPATK's mandate is international cooperation. The organization's head, Ivan Yustivandana, noted that PPATK "is coordinating internationally with the FIUs of other countries" in identifying illegal flows of investment funds.(Hutasoit, 2022) In the same interview, he shared that they have exchanged information on 150 unlicensed online lenders to

the financial sector so all will now monitor their transactions.(Berita Kota, 2021) To verify any evidence of cross-border laundering, PPATK's work also includes ensuring Indonesian banks or financial technology (fintech) providers report any foreign funds to PPATK in compliance with Indonesian legislation. Thus even if Ponzi or illegal investment schemes incense where there is an existent overseas fund transfer (such as crypto schemes), PPATK can correlate the crossings and "mark" it under relevant AML legislation. It is worth noting that PPATK performs its functions based on international AML legislation (under international conventions and the protocol under the Egmont Group). In short, PPATK is the cornerstone of financial intelligence. Law No. 8 of 2010 provides it great power in that it can "intercept" and in cases "freeze" and "retain" payment amounts that are suspect, and even liaise with other regulators across borders. PPATK coordination at this level, both nationally and internationally, has already resulted in the largest amounts seized from Ponzi operators to date, showing how transnational schemes are targeted and monitored under PPATK guidelines.

In addition to PPATK, the Commodity Futures Trading Regulatory Agency (Bappebti), which is under the Ministry of Trade has a role as well. Bappebti is responsible for the oversight of markets for commodities and derivatives, including cryptocurrency trading. Ponzi-like frauds that intersect this market are defined by Indonesian law. Law No. 10 of 2011 (amending the 1997 futures law) makes it illegal for any person to provide futures or derivative contracts "with or without promotion or recruitment or training etc." without being registered or licensed by Bappebti. With this broad terminology, Ponzi operators that claim to be commodity investment or crypto investment platforms are criminalized. In fact, a no person operating as a futures trader without being registered in violation of Article 49(1a) of that law faces severe consequences: Article 73D makes an unlicensed futures trading activity punishable by 5 to 10 years imprisonment as well as a fine of up to IDR 20 billion (≈ EUR 1.05 million). Thus, a crypto Ponzi or multi-level marketing scheme is captured by this ban on commodity trading if they marketed themselves as a trading contract. More generally, the Trade Minister’s Law No. 7 of 2014 specifically prohibits pyramid schemes: Article 9 prevents any arrangement for pyramid marketing. For example, the 2021 Edccash crypto-Ponzi had charges filed against it according to Article 9 of Law No. 7 of 2014 as a banned pyramid distribution of goods. This statutory language creates clear authority for Bappebti and other agencies. They could say many Ponzi schemes are illegal futures/dealing or pyramid marketing, which both carry long prison sentences for violations. (After Jan 2025, OJK obtained crypto market oversight via new

regulations but the crimes are still the same.) Consequently, Bappebti and the Trade Ministry laws fill a lot of legal holes – establishing together that any Ponzi or money-game scheme disguised as trading/investing is countenanced only if it has regulatory approval, otherwise it is criminal.

Furthermore, Bank Indonesia (BI), which is Indonesia's central bank, likewise supports the framework. BI's role against fraud is mainly through its assurances of cooperation in the banking sector and implementing AML provisions (BI used to have the Financial Intelligence Unit before the existence of PPATK). Being that BI regulates payment systems it can help identify large illicit transactions. Working with the directives of OJK, the commercial banks, whom BI supervises solvency, have helped freeze the suspected Ponzi funds. For example, OJK stated that multiple banks blocked fraud accounts at once. OJK told all banks to block accounts listed by other banks. BI also requires diligence of customers; according to Law No. 7 of 2011 (Banking Law) banks must screen transactions and report suspicious activity to PPATK. Although BI does not have a specific Ponzi framework, BI set forth certain banking regulations and when combined with OJK and Satgas PASTI (the financial crimes task force) the banking system should relay those suspicious investment related flows to the authorities for investigations.

Operationally, it has strengthened inter-agency and cross border cooperation. Domestically, OJK, BI, PPATK, Bappebti, Kominfo, the police and other ministries cooperatively work together through committees. For instance, the Investment Alert Task Force *(Satgas Waspada Investasi)* hold meetings on a regular basis to share and report intelligence with each other. Kominfo blocks fraudulent websites and apps, reportedly thousands of illegal investment domains have been blacklisted in 2022 (with illegal forex and Ponzi sites being the highest on the list). OJK's 2022 press release referred to "cyber patrol and daily blocking together with the Ministry of Communication and Informatics (*Kementerian Komunikasi dan Informatika*, Kominfo)" to minimize the online space operated by illegal lenders.(Otoritas Jasa Keuangan, 2022) Internationally, Indonesia's MOUs and Interpol channels have been leveraged. PPATK participates in the Egmont Group of FIUs and exchanges suspicious transaction reports with a number of foreign partners.(Bintoro et al., 2021) In practice, PPATK has traced flows involving other countries (e.g. provide banks with instructions to report foreign related transfers) and Indonesian prosecutors work with their foreign counterparts when cyber

scammers flees abroad or hut resumes originating from local accounts are stashed in an offshore account. As part of the ongoing effort to stop abuse, authorities hold public awareness campaigns - OJK is active in educating consumers about the red flags for scams through social media and outreach to local communities - to make potential victims less susceptible to cross-border Ponzi motivations.(Kasim et al., 2025)

Jurisdictional Challenges in Cross-Border Ponzi Prosecutions

Indonesian criminal jurisdiction is governed in theory by a several available principles. First, regarding territoriality, it is established under KUHP Article 2, which asserts criminal jurisdiction over "any person who commits a crime in Indonesia" (KUHP Art. 2(1)). Second, the active nationality principle (KUHP Article 5), provides that Indonesian law will cover offences committed by Indonesian citizens in other parts of the world, and to be covered, the act must be (1) "punishable under Indonesian law and also a crime in the country in which they were committed (KUHP Art. 5(1)). Third, the passive/protective principle takes account of foreign offences committed abroad that do harm to Indonesia, particularly offences that are "aimed at disrupting Indonesia’s national security, economic interests, or any other interests of the state which are considered vital" (KUHP Art. 7(1)). Ultimately, in theory these doctrines mean that, if for example, an Indonesian citizen runs a Ponzi scheme overseas (which could apply to KUHP Art. 5), or a foreign citizen’s Ponzi scheme directly harms Indonesian victims or state interests (which could apply to KUHP Art. 7), the Indonesian courts could claim jurisdiction.

In applying these concepts to a cyber-enabled Ponzi scheme, the practical aspect poses challenges. Although Ponzi schemes arguably date back to the beginning of time, and Ponzi schemes are certainly not new (but no doubt they have historically been a popular vehicle of fraud), while most modern-day Ponzi schemes are operated and organized online, the complexity addresses the premise of where the crime occurs, and therefore, that state's law applies. For example, if a group of fraudsters is operating a Ponzi scheme from a cloud server and enticing victims through social media across the globe, it will be nearly impossible to even determine where the "place of the offense" is located. While the perpetrator isn't in Indonesia and the only connection to the crime is Indonesian victims, it is still unclear whether it could even fall under passive-protective jurisdiction principles. As Simon Butt (2023), has pointed out, Indonesia's theory of active nationality "follows its nationals wherever they go," but only

to the limit it chooses to exercise that right, and it likely would not exercise it if the foreign country has prosecuted the offender.(Butt, 2023) The protective principle does technically apply to crimes committed by foreigners that are injurious to Indonesia, but it is also rarely been tested in practice in cases of financial fraud. Therefore, although articles 2, 5 and 7 of the KUHP present legal bases for jurisdiction, the multi jurisdictional nature of Ponzi schemes means that Indonesian law enforcement can rarely assert unilateral jurisdiction without significant cooperation through the international legal framework.

Indonesian legal authorities are increasingly willing to use international collaboration in responding to transnational Ponzi schemes. A high-profile illustration of this trend is a recent case that involved a network based in Malaysia that defrauded Indonesian victims. The Jakarta police arrested two suspects - one Indonesian and another Malaysian- in May 2022 for operating an app called 'Morgan Asset Group' that promised investors 150% returns. Investigators determined that the scheme was controlled from Malaysia, so following the arrest of both suspects (under Indonesia's electronic information and fraud laws), police filed charges and coordinated with Interpol and the Malaysian authorities to pursue the rest of the ringleaders who were still at large in Malaysia. The Kuala Lumpur-based operators had recruited victims in Indonesia via Facebook. They concealed the investment scheme's true nature, routed funds from Indonesian victims to Indonesian bank accounts, and this allowed the police to charge the arrested suspects under Indonesia's ITE Law (Article 45A) or KUHP fraud (Article 378) and money laundering statutes. The Indonesian authorities are explicit about the cross-border aspect: they are *'berkoordinasi dengan Interpol untuk membongkar sindikat penipuan ini yang berada di Malaysia'* (coordinating with Interpol to break up this Malaysian fraud syndicate).(Imam, 2025)

In addition to dealing with individual cases, Indonesia has taken part in broader multinational efforts to disrupt Ponzi fraud. For example, the tax enforcement agencies from the five major economies (the "J5" group) of the world have recently shared around a billion dollars that was lost to investment fraud, cooperated on intelligence on global cryptocurrency crimes, and identified leads on a billion-dollar global Ponzi scheme that involved every jurisdiction represented in the J5 (Canada, the USA, Great Britain, Australia, and the Netherlands).(Khairizka, 2022) This is one way transnational fraud can emerge from multinational information-sharing. UN agencies have also educated Indonesian investigators

about financial crime networks and how “financial crimes often have cross-border elements”, including the mutual legal assistance (MLA) process that is often necessary to collect evidence. Yet they note that, despite the existence of laws on MLA, if Indonesia does seek evidence from other jurisdictions in a financial crime case, the process can be slow, which is why they often use more informal sources of intelligence, contacts, and relationships with other officials in other agencies, or industry contacts who may have first-hand knowledge or awareness of the case, and can deliver evidence quicker.(United Nations Office on Drugs and Crime, 2025) Government agencies and departments, and prosecutors and investigators, engaged in actual enforcement action against transnational Ponzi schemes in Indonesia, now regularly rely on collaboration with foreign partners, whether through treaties, INTERPOL coordination,(Associated Press, 2024) or multilateral agency forums, so that they can collect evidence offshore, and establish jurisdiction over foreign individuals and businesses.

Furthermore, collecting evidence on transnational Ponzi schemes poses another layer of difficulty. Most of the evidence - server logs, transaction records, witness accounts, bank account records - are often not in Indonesia. Indonesian investigators do not have power to obtain data held outside the country which is also the case with compulsion from witnesses based outside Indonesia. On paper though, the Mutual Legal Assistance Act (Law No. 1 of 2006) provides tools for international cooperation. Article 3 of this legislation allows for requests for assistance including obtaining documents, executing a search and seizure warrant from another country, freezing assets and moving evidence needed, again subject to domestic law of the requested country. In practice though, each request goes through strict MLAT (mutual legal assistance treaties) or diplomatic channels that take a number of months or sometimes years. Even then, countries will assist to the extent that the crime alleged is also a crime under their domestic law (the notion of dual criminality), and there are still some forms of digital evidence which may be treated at a minimum as private, or may have to be obtained with a court order from abroad.

Academics discuss a mismatch between the crime and enforcement environment: Josua Sitompul states, "cybercrime has no borders and the cyberspace is an un-territorialized domain," but investigators operate within national sovereignty.(Sitompul, 2020) A Ponzi scheme operator could be using digital platforms worldwide, and could have stored the transaction data on servers in Singapore or the US, which are beyond Indonesian jurisdiction. In establishing a data

access regime in Indonesia, it is relevant to note that Indonesia is not a party to the Budapest Cybercrime Convention, so it is without a mechanism for preserving or production orders to foreign tech companies, let alone all the intermediaries. For that reason, authorities generally rely on the (very formal) MLAT process, through Interpol, or if they are lucky, they may have a bilateral law enforcement partner. Indonesia's recent experience cooperating with the UNODC in a workshop reported at the MLA "remains key to the evidence gathering process", but in actuality agencies "have to work around knowing an MLA will take time really learning the best way to leverage professional connections to get a timely response about what you need".(United Nations Office on Drugs and Crime, 2025) For example, if an Indonesian investigator was cooperating informally with Malaysian or Singaporean investigators, the possibility exists for them to act quickly to freeze assets or copy server data that is used from the tech company servers before the MLAT reply arrives from the tech company's home country. Such non-legal diplomatic cooperation assists to close the gap on the time frames involved in the legal-based time frames.

Another procedural issue is dealing with the boundaries set forth by privacy laws. Indonesia's new Personal Data Protection Law (2022) has new rules about cross-border transfers of personal data when conducting business outside of the country. Regarding criminal cases, this means that requesting financial and personal records in operational cases from foreign banks, or tech platforms, may require complying with both Indonesian PDPL requirements and the privacy laws of that foreign country. This can further will delay evidence gathering for prosecutors. Furthermore, Indonesian prosecutors will have to present a case with sufficient evidence to satisfy evidentiary standards in Indonesia - to demonstrate that a fraudulent scheme was committed under Indonesian doctrine of criminal law, even if almost all evidence originates from the foreign country. Addressing all of these procedural issues simply means that the evidence will be neither timely data nor exhaustive information when a case is finally ready for trial.

Institutional Capacity Constraints in Combating Cyber-Enabled Ponzi Schemes

The struggle against cyber-based Ponzi schemes in Indonesia represents significant institutional capacity constraints particularly related to digital forensics and cybersecurity. According to Izazi Mubarok, Chairman of the Indonesian Digital Forensic Association

(*Asosiasi Forensik Digital Indonesia*, AFDI), Indonesia suffers from a number of cybersecurity professionals, but this impacts the ability of institutions to protect their systems and for them to respond appropriately in the event of a cybersecurity incident. The problem is not only quantitative as there is a lack of highly skilled professionals in the field of digital forensics, which requires up-to-date technical skills and knowledge and legal frameworks. In this context the certification is becoming an important indicator of competence. Practitioners can be a standard measure of competence by achieving external recordable certifications, known international certifications such as CHFI (Computer Hacking Forensic Investigator), GCFA (GIAC Certified Forensic Analyst), EnCE (EnCase Certified Examiner) and CFCE (Certified Forensic Computer Examiner). Unfortunately, the access to and availability to these certifications in Indonesia is very limited, leaving a limited pool of quality experts.(Xynexis, 2025)

Experts like Muhammad Nur al-Azhar point out that the lack of digital forensic specialists in Indonesia is compounded and made worse due to the accelerating growth and complexities of digital data. The increasing complexity and sophistication of cybercrimes like digital Ponzi schemes require the ability to evolve forensic methodologies. Yet, there is questionable ability in understanding how cyber attacks happen and where it originates from. Thomas Gregory, Director of Blue Team Operations, at PT Spentera emphasizes that not being able to point to the culprit of a cyber incident is manifesting symptom of the insufficient application of digital forensics that the country is incorporating. Moreover, the difficulty of doing digital forensics work is complicated with legal conditions. Under Article 6 of the Electronic Information and Transactions Law of Indonesia, forensic experts need to make sure that electronic documentation used as evidence must be available, displayed, comprised, and accounted. The legal liability entails that a forensic practitioner not only has knowledge and understanding of such work, they need to demonstrate a reasonable and high practical ability to perform any forensic act. For instance, they need to be able to explain what a digital file was, where it was, what it is used for and for what sector it represents. They also must be able to explain its forensic provenance, hash value, and how they analyzed it when testifying regarding the file in court.(Teknobuzz, 2024)

Moreover, the professional ecosystem surrounding digital forensics is still developing. AFDI, which comprises members from government institutions (such as Police, Prosecutors, the Corruption Eradication Commission, the Supreme Audit Board (*Badan Pemeriksa*

Keuangan, BPK), and the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*, BSSN)), academia, private sectors, and civil society, currently has around 300 members. However, this number is insufficient to meet the growing demands posed by the proliferation of cybercrime.(Atmaja, 2021) Dani Prawira - a Senior Associate with Assegaf Hamzah & Partners stated that Indonesia is seeing a short supply of digital forensic professionals. Historically, digital forensic experts have been involved with the collection of the electronic evidence and have taken that through to the courtroom. Today, digital forensic experts are gaining more roles and demand - from the private sector, not just law enforcement. While the demand from the police and prosecutors for digital forensic experts remains, only a few of the universities provide digital forensics as a formal area of study, leading to a low number of professionals in the field, and creating a supply bottleneck as a part of the larger effort to combat cyber-based Ponzi schemes.(Kencana, 2020)

On the undergraduate level there is no university offering a standalone bachelor's degree in digital forensics. Some universities and colleges, such as Telkom University and Universitas Udayana,(Forensik Digital, 2019) include bits and pieces of digital forensics in their other degrees or programs, like Information Technology or Informatics, but these components are typically minor, elective, or minor courses. On the graduate level, Telkom University offers a wholly new master's degree in Cyber Security and Digital Forensics, which is the first master's degree specific to digital forensics in Indonesia. It began in 2021.(Telkom University, 2021) Additionally, Universitas Islam Indonesia (UII) offers a digital forensics concentration in its Masters of Informatics with one of the few master's programs that brings digital forensics into higher education.(Jurusan Informatika UII, 2025) Since there are no comprehensive or specialized undergraduate education and training pathways, there are few graduates of higher or further education that enter the workforce that have the necessary knowledge and expertise in digital forensics.

A report has recently confirmed a notable uptick in cybercrime in Indonesia. More specifically, the growth of online fraud and identity theft is evident. According to VOI's analysis of data sourced from the public license and Internet identity theft and fraud reports for 2023, it was found that online fraud cases made up 32.5% of all total cybercrime cases - which reflects an increase of 10.3% from the period before the year analyzed. Additionally, in 2022 identity theft cases were at 7.96%, which jumped to 20.97% in 2023.(Putri & Julianto, 2024) This causes

a critical and responding threat to public security, or national security in the realm of cyberspace. Despite the rise of online fraud and cybercrime, the willingness, capacity, and capabilities of law enforcement agencies, which can be delimited pure law enforcement forces, special agencies which take on an enforcement role to the law, and or National Security council have been expected or needed to react and respond to the above-mentioned responses from our public, fast growing. Timely investments into resources, training, and institutional capabilities will not only help to meet growing cyber-risks, but also assistance and provision to individuals and organizations to reduce their vulnerability to cyber vulnerability exploitation.

Complexities of Digital Evidence and Anonymity in Transnational Digital Ponzi Scheme

Even when the personnel are in place, digital forensic investigations can be challenged by seemingly insurmountable data problems. Modern Ponzi schemes generate huge amounts of digital evidence. In fact, Indonesia saw its crypto trading volume grow from IDR 60 trillion (≈ EUR 3.18 billion) in 2020 to IDR 859 trillion (≈ EUR 45.53 billion) in 2021 which means there was an incredible amount of transactional data to analyze.(Reuters, 2022) Investigators have to review and analyze massive blockchain ledgers, trading records, and correspondence and communications logs to determine how the money flowed. Ultimately, it is this high volume of data, and the complexity of that data, as it sometimes requires investigators to analyze potentially a bigger volume of data than they have available in time and processing capabilities. Investigators and analysts might be in a position to retrieve and analyze a large series of gigabytes or terabytes of data from a variety of sources – from server/hosting backups to other devices of the user periphery or reporting – which can either be time-consuming or draw on resources they may not even have available.

Nonetheless, the data of bitcoin and cryptocurrency are volatile. Unlike physical evidence, digital evidence can be manipulated and deleted where suspects can destroy devices, reset servers, and rapidly transfer funds through different cryptocurrency exchanges and wallets. Cybercriminals take advantage of the instability of bitcoin and cryptocurrency by laundering revenue from crime through several blockchain networks within minutes or obfuscating the trail through "mixers". Law enforcement also points out that the overwhelming "volume of transactions" combined with the use of layering means it is harder for governments to track and combat illicit flows of money.(Zellers, 2024) The way the crypto space is moving at present means that the issue of crypto being accepted quickly by Indonesia is a big problem.

The government thinks about crypto in terms of a financial asset but not for payments, and therefore the criminals will find a way to take advantage of this gap. Transaction volume is staggering! In May 2025 Indonesia had an estimated volume of IDR 49.57 trillion (approx. EUR 2.62 billion) of crypto trades,(Jakarta Globe, 2025) having had an average of between 1.2 to 1.6 trillion of IDR or approx. EUR 63 million to EUR 85 million (first quarter of 2025) daily, and a total IDR of 109.29 trillion (approx. EUR 5.78 billion) in the first quarter of 2025.(Indonesia Crypto Network, 2025) Globally, it was reported that a total of USD 14 billion of cryptocurrency was lost to fraud worldwide in 2021 which was a 79% increase from the previous year,(Chainalysis, 2022) with Indonesia being considered "a significant hotspot" for money laundering using crypto. It is essential to enhance the supervision as volumes increase and the regulations develop in order to mitigate risk of illicit activities.

Moreover, the situation has become even more complicated because Ponzi schemes are increasingly leveraging encryption and privacy technology to obscure their tracks. There is a considerable amount of communication that occurs between offenders and victims via end-to-end encrypted messaging applications (WhatsApp, Telegram, etc.) and private or semi-private forums, many of which do not allow for any traceable data to be recovered unless a device is seized quickly or a key is obtained rapidly.(Terenzi, 2025) Perpetrators of fraud can also exploit virtual private networks (VPNs) and anonymizing browsers (such as Tor) to mask their online presence.(Jain et al., 2025) From a financial standpoint, fraud operators prefer to conduct transactions in cryptocurrencies and stablecoins that allow for at least a degree of pseudonymity. As discussed in Binance analysis of regional fraud, Tether (USDT) on the Tron blockchain seems to have rapidly become "the first choice of Asian criminal groups" for storing and laundering their illicit profits. Indonesian investigators at first had difficulty with this trend; as one of their studies noted, Thai investigators who were confronted with a similar wave of crypto-scams in their country "faced difficulties because of the anonymity of cryptocurrency transactions and the complexity of the blockchain" before launching into deployments of specialized analysis platforms. Cryptocurrencies often are not investigated or forfeited through traditional financial investigations as investment fraud and financial fraud typically are. Unless there are advanced blockchain tracing tools and trained blockchain personnel to identify and trace the transaction, forensic examination of cryptocurrency transactions in Ponzi schemes remains a considerable bottleneck.(Binance, 2024)

Alongside Crypto, modern Ponzi schemes use social media and online networks to recruit investors and to obscure the reality of their operations. Indonesian scam promoters typically present an ostentatiously respectable online presence, particularly to imply legitimacy. Actually, there are scammers who can tap into mass audiences at low cost through platforms such as Instagram, Facebook, YouTube, and Telegram. One recent example showed, as recently as 2020, the scheme "mentors," using well over 200,000 members on Telegram for one Ponzi app and that group alone contained information that spread referral links and investment tips which appealed to thousands of victims in a matter of days.(Llewellyn, 2022) Scamming promoters can also use paid ads, fake testimonials, and follow the pack by getting celebrities to endorse their scams online to build credibility. The ability of law enforcement to monitor and investigate this ecosystem is limited by manpower, as well as technology gaps which hinder their abilities. Research by Haq et al (2023) shows that Indonesian cyber units have "not optimized" their strategies to detect techniques and exploits on social media due to resource constraints and continue to note massive amounts of worthless fraudulent activity created on behalf of scam operators.(Haq et al., 2023)

Dhali et al (2023) research also shows that online forums and darknet markets are also one of the recruiting mechanisms for cryptocurrency Ponzi schemes due to a higher level of anonymity. Investigators will deal with stolen data traded in these underground spaces and public messaging that disappears without a trace sometimes seconds after being posted.(Dhali et al., 2023) Study by Guan (2024) reveals that the rapidity of social media influences even more so because schemes can gain critical mass before any of the authorities have been alerted to its existence by the time people report it, the assets may have already been transferred offshore.(Guan, 2024) This illustrates the disadvantage posed by social networking tools and crypto platforms relatively speaking to fraudsters, simultaneously elevating the hurdles for humans investigators and also forensic analysts.

CONCLUSION

Indonesia's experience with cross-border Ponzi schemes emphasizes the complicated set of relationships between changing methods of digital fraud and institutional capacity to respond. The country has a double whammy: a growing pool of potentially vulnerable investors - especially youth invested in crypto trading - and increasingly sophisticated fraud operations that apply various iterations of digital technology and take advantage of anonymity across borders.

Although Indonesia has established a legal framework to deal with emulating Ponzi schemes as potential subject to prosecution through criminal, banking, capital market and/or trade laws, the subsequent enforcement actions are currently challenged with the jurisdictional aspects, forensic capacity and speed of co-operation by countries outside Indonesia. Agencies seem to be responding in ways - like freezing assets, warning consumers, or engaging in cooperation - through OJK, PPATK, Bappebti cooperation, but these responses developed after the Ponzi schemes-operationalized swiftly and can be enhanced to conduct coordinated approaches to coordinating an effective usage of digital platforms more generally but exploiting regulatory change.

The recent legislative reform and participation in global financial intelligence networks suggest that Indonesia is on the path toward enhanced legal congruity and international cooperation. There remain human resourcing gaps, few to no digital forensic capabilities, and limited investigative capacity that inhibit the State's ability to disrupt these schemes proactively. Without an offsetting amount of community-wide capacity building investment, especially in digital forensics, the legal tool kit will go under-utilized. Ultimately, reforming legal instruments will certainly upgrade the effort to combat transnational Ponzi schemes, but Indonesia must add operational readiness, regional and global coordination, and public awareness investments to inoculate their people against the continuing maturation of financial fraud.

ACKNOWLEDGEMENT

The author would like to express sincere gratitude to Prof. Krisztina Karsai for her invaluable insight, guidance, and unwavering support throughout the research process. Her expertise and constructive feedback were instrumental in the development and completion of this article.

REFERENCES

Abid, G., & Ahmed, A. (2014). Failing in corporate governance and warning signs of a corporate collapse. *Pakistan Journal of Commerce and Social Sciences (PJCSS)*, *8*(3), 846–866.

Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics:

Investigating crypto frauds. *International Journal of Network Management*, *34*(2). https://doi.org/10.1002/nem.2255

Aki, J. (2024, October 28). *Over 60% of Young Indonesians Invest in Crypto: Report*. Cryptonews. https://cryptonews.com/news/over-60-of-young-indonesians-invest-in-crypto-report/

Aprian, D. (2024, November 1). *Crypto Transaction Reaches IDR 426 Trillion, Mobee Also Encourages Crypto Industry Development*. VOI; VOI.ID. https://voi.id/en/economy/430349

Arya, N. (2025, March 19). *Online Fraud Using Stock and Crypto Trading Mode Revealed, Losses Reach IDR 105 Billion*. Kompas. https://www.kompas.id/artikel/en-penipuan-daring-bermodus-perdagangan-saham-dan-kripto-kerugian-tembus-rp-105-miliar

Associated Press. (2024, October 10). *Indonesia arrests suspect wanted by China for running $14 billion investment scam*. VOA. https://www.voanews.com/a/indonesia-arrests-a-suspect-wanted-by-china-for-running-a-14-billion-investment-scam/7818080.html

Atmaja, B. T. (2021, December 16). *Ahli Forensik Digital Itu Berat Tugasnya*. Cyberthreat.Id. https://cyberthreat.id/read/13065/Ahli-Forensik-Digital-Itu-Berat-Tugasnya

Bartoletti, M., Pes, B., & Serusi, S. (2018). Data Mining for Detecting Bitcoin Ponzi Schemes. *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 75–84. https://doi.org/10.1109/CVCBT.2018.00014

Berita Kota. (2021, October 27). *PPATK Ungkap Skema Ponzi dalam Praktik Pinjol Ilegal*. Berita Kota. https://beritakota.id/ppatk-ungkap-skema-ponzi-dalam-praktik-pinjol-ilegal/

Binance. (2024, October 15). *Report Interpretation | UNODC releases fraud report on transnational organized crime in Southeast Asia*. Binance. https://www.binance.com/en/square/post/14891641668673

Bintoro, S., Sjamsuddin, S., Pratiwi, R. N., & Hermawan, H. (2021). Prevention Policies for Money Laundering through Capital Market Instruments: The Case of Indonesia. *The Journal of Asian Finance, Economics and Business*, *8*(2), 1269–1275.

Boshmaf, Y., Elvitigala, C., Al Jawaheri, H., Wijesekera, P., & Al Sabah, M. (2020). Investigating MMM Ponzi Scheme on Bitcoin. *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2020*, 519–530. https://doi.org/10.1145/3320269.3384719

Butt, S. (2023). Indonesia's new Criminal Code: indigenising and democratising Indonesian criminal law? *Griffith Law Review*, *32*(2), 190–214. https://doi.org/10.1080/10383441.2023.2243772

Chainalysis. (2022). *Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity*. Chainalysis. https://www.chainalysis.com/blog/2022-crypto-crime-report-introduction/

Chavez-Dreyfuss, G. (2019, April 30). *Cryptocurrency thefts, fraud hit $1.2 billion in first quarter - report*. Reuters. https://www.reuters.com/article/business/cryptocurrency-thefts-fraud-hit-12-billion-in-first-quarter-report-idUSKCN1S62P0/

Chen, J. (2024, January 26). *Ponzi Scheme: Definition, Examples, and Origins*. Investopedia. https://www.investopedia.com/terms/p/ponzischeme.asp

Commodity Futures Trading Commission. (2023). Federal Court Orders South African Company to Pay Over $1.7 Billion in Restitution for Forex Fraud | CFTC. In *Commodity Futures Trading Commission*.

Dhali, M., Hassan, S., Mehar, S. M., Shahzad, K., & Zaman, F. (2023). Cryptocurrency in the Darknet: sustainability of the current national legislation. *International Journal of Law and Management*, *65*(3), 261–282. https://doi.org/10.1108/IJLMA-09-2022-0206

Forensik Digital. (2019). *Digital Forensik*. Forensik Digital. https://forensikdigital.com/digital-forensik/

Guan, S. S. (2024). Fraud on the Social Media Market Essays. *Northwestern University Law Review Online*, *119*, 206–221.

Gupta, M. (2024). Negative impact of Ponzi Schemes on Crypto-market. *Scientific Journal of Metaverse and Blockchain Technologies*, *2*(2), 32–42. https://doi.org/10.36676/sjmbt.v2.i2.30

Haq, M. A., Barthos, M., & Fakrulloh, Z. A. (2023). Digital forensics in online fraud crimes investigation. *Proceedings of the 3rd International Conference on Law, Social Science, Economics, and Education*, 50.

Hidajat, T. (2018). Financial literacy, Ponzi and pyramid scheme: evidence from Indonesia. *Journal of Economic & Management Perspectives*, *12*(1), 193–200.

Hutasoit, M. (2022, April 5). *PPATK Blocks 345 Accounts Related To Illegal Investments, The Value Is Over Half A Trillion*. VOI. https://voi.id/fr/berita/153884

Imam, R. (2025, May 2). *Polisi Tangkap 2 Pelaku Investasi Bodong Jaringan Malaysia, Korban Rugi Rp 18 M*. Kumparan. https://kumparan.com/kumparannews/polisi-tangkap-2-pelaku-investasi-bodong-jaringan-malaysia-korban-rugi-rp-18-m-24zWiKTzoDW

Indonesia Crypto Network. (2025, May 5). *Indonesia's Crypto Transactions Hit IDR 109.29 Trillion in Q1 2025*. Indonesia Crypto Network. https://indonesiacrypto.network/blog/indonesias-crypto-transactions-in-q1-2025

Isaac, J. (2025, May 26). *OJK uncovers massive online scam, launches anti-fraud center*. Indonesia Business Post. https://indonesiabusinesspost.com/4374/financial-crimes/ojk-uncovers-massive-online-scam-launches-anti-fraud-center

Jain, V. K., Aggrawal, J., Dangi, R., Prasad Shukla, S. S., Yadav, A. K., & Choudhary, G. (2025). Unmasking the True Identity: Unveiling the Secrets of Virtual Private Networks and Proxies. *Information*, *16*(2), 126. https://doi.org/10.3390/info16020126

Jakarta Globe. (2025, July 11). *COIN Hits Limit Up for Three Days Since Market Debut*. Jakarta Globe. https://jakartaglobe.id/special-updates/coin-hits-limit-up-for-three-days-since-market-debut

Jurusan Informatika UII. (2025). *Concentrations and Courses Offered by the Master of Informatics Study Program for Professional*. Jurusan Informatika UII. https://informatics.uii.ac.id/curriculums-profesional/

Kasim, E. S., Muda, S., Md Zin, N., Mohd Padil, H., Ismail, N., & Syed Yusuf, S. N. (2025). Combating investment scams: insights from law enforcement and civil society toward a prevention framework. *Journal of Criminological Research, Policy and Practice*. https://doi.org/10.1108/JCRPP-04-2025-0030

Kencana, M. R. B. (2020, February 24). *Minim Jumlah, Indonesia Butuh Banyak Tenaga Ahli Digital Forensik*. Liputan 6. https://www.liputan6.com/bisnis/read/4186777/minim-jumlah-indonesia-butuh-banyak-tenaga-ahli-digital-forensik?page=2

Khairizka, P. N. (2022, May 23). Potensi Skema Ponzi, Belanda Hingga AS Saling Tukar Data Kriminal Kripto. *Pajakku*.

Lensburg, C. (2024, August 19). *Report: The Highly Effective Deployment of Cryptocurrencies in MLM- and Ponzi Schemes! | FinTelegram News*. Fintelegram. https://fintelegram.com/report-the-highly-effective-deployment-of-cryptocurrencies-in-ponzi-schemes/

Liu, X., Huang, F., & Yeung, H. (2018). The regulation of illegal fundraising in China. *Asia Pacific Law Review*, *26*(1), 77–100. https://doi.org/10.1080/10192557.2018.1511086

Llewellyn, A. (2022, May 10). *'Crazy rich' Indonesians' arrests spotlight investment perils*. Aljazeera. https://www.aljazeera.com/economy/2022/5/10/crazy-rich-indonesians-arrests-spotlight-investment-perils

Lyngaas, S. (2023, April 11). *Inside the international sting operation to catch North Korean crypto hackers*. CNN. https://edition.cnn.com/2023/04/09/politics/north-korean-crypto-hackers-crackdown/index.html

Monroe, H., Carvajal, A., & Pattillo, C. (2010). Perils of Ponzis. *Finance and Development*, *47*(1).

Mugarura, N. (2017). The use of anti-money laundering tools to regulate Ponzi and other fraudulent investment schemes. *Journal of Money Laundering Control*, *20*(3), 231–246. https://doi.org/10.1108/JMLC-01-2016-0005

Otoritas Jasa Keuangan. (2015). *Press Release: Be Cautious with Cyber Crime and Potentially Unfavorable Investment Offers*. Otoritas Jasa Keuangan. https://ojk.go.id/en/kanal/edukasi-dan-perlindungan-konsumen/berita-dan-kegiatan/siaran-pers/Pages/press-release-be-cautious-with-cyber-crime-and-potentially-unfavorable-investment-offers.aspx

Otoritas Jasa Keuangan. (2016). *OJK Takes Part Again in IOSCO GEM-C 2016 Forum*. Otoritas Jasa Keuangan. https://ojk.go.id/en/kanal/pasar-modal/berita-dan-kegiatan/info-terkini/Pages/OJK-Takes-Part-Again-in-IOSCO-GEM-C-2016-Forum.aspx

Otoritas Jasa Keuangan. (2022). *Satgas Waspada Investasi Kembali Temukan 10 Entitas Investasi Ilegal dan 100 Pinjaman Online Ilegal*. Otoritas Jasa Keuangan. https://ojk.go.id/waspada-investasi/id/siaran-pers/Pages/Satgas-Waspada-Investasi-Kentitas-Investasi-Ilegal-dan-100-Pinjaman-Online-Ilegal.aspx

Pratama, M. R. Y., Muriman, C., & Nita, S. (2025). Establishing the Legal Basis for Crypto Asset Confiscation: A Critical Study on the Challenges of Cybercrime Law Enforcement in Indonesia. *Policy, Law, Notary, and Regulatory Issues*, *4*(2 SE-Articles), 284–298. https://doi.org/10.55047/polri.v4i2.1679

Putri, D. B., & Julianto, A. (2024, February 1). *Online Fraud Becomes The Most Cyber Susceptibility Case In 2023*. VOI. https://voi.id/en/technology/353311

Raidi. (2025, March 21). *Indonesian Police Uncover Rp105 Billion International Crypto Investment Scam*. Indonesia Sentinel. https://indonesiasentinel.com/indonesian-police-uncover-rp105-billion-international-crypto-investment-scam/

Reuters. (2022, January 25). *Indonesia regulator says financial firms banned from facilitating crypto sales*. Reuters. https://www.reuters.com/world/asia-pacific/indonesia-regulator-says-financial-firms-banned-facilitating-crypto-sales-2022-01-25/

Scharfman, J. (2023). Cryptocurrency Ponzi, Pyramid, and MLM Schemes: Part 1. In J. Scharfman (Ed.), *The Cryptocurrency and Digital Asset Fraud Casebook* (pp. 35–53). Springer International Publishing. https://doi.org/10.1007/978-3-031-23679-2_3

Seoul, P. V. in N. Y. and E.-Y. J. in. (2020, February 8). *Cryptocurrency Scams Took in More*

Than $4 Billion in 2019. Wall Street Journal. https://www.wsj.com/articles/cryptocurrency-scams-took-in-more-than-4-billion-in-2019-11581184800

Setiawan, P. J., & Ardison, H. (2021). Criminal Victimization on Large-Scale Investment Scam in Indonesia. *Veritas et Justitia*, *7*(1), 1–30. https://doi.org/10.25123/vej.v7i1.3917

Sitompul, J. (2020). *Cross-border Access to Electronic Evidence: Improving Indonesian Law and Practice in Investigating Cybercrime*. Koninklijke Boom uitgevers.

Suwitho, S., Budi Riharjo, I., & Ary Dewangga, D. (2023). The nexus between Ponzi scheme and multi-level marketing systems: Evidence in Indonesia. *Cogent Social Sciences*, *9*(1), 1–17. https://doi.org/10.1080/23311886.2023.2178540

Teknobuzz. (2024). *Indonesia Kekurangan SDM Forensik Digital*. Teknobuzz. https://teknobuzz.id/2024/08/04/indonesia-kekurangan-sdm-forensik-digital/

Telkom University. (2021). *Tel-U Menjadi Kampus Pertama Dengan Program Studi S2 Digital Forensic & Cyber Security*. Telkom University. https://telkomuniversity.ac.id/tel-u-menjadi-kampus-pertama-dengan-program-studi-s2-digital-forensic-cyber-security/

Terenzi, M. (2025). Cryptocurrencies from Mainstream to Fringe Platforms. Media Manipulation and Deceptive Schemes on Facebook and Telegram. *Comunicazione Politica*, *26*(1), 93–120.

U.S. Attorney's Office. (2023). *Indonesian National Extradited from Singapore to Face Charges of Running Ponzi Scheme Targeting Indonesian and Indo-American Community*. U.S. Attorney's Office. https://www.justice.gov/usao-edny/pr/indonesian-national-extradited-signapore-face-charges-running-ponzi-scheme-targeting

United Nations Office on Drugs and Crime. (2025). *Indonesia strengthens financial investigation capabilities to fight corruption*. United Nations Office on Drugs and Crime. https://www.unodc.org/roseap/en/indonesia/2025/02/financial-investigation-fight-corruption/story.html

Weisman, S. (2020, August 12). *The History of Ponzi Schemes Goes Deeper Than You Think*. Time. https://time.com/5877434/first-ponzi-scheme/

Xynexis. (2025). *Membangun Karier di Dunia Digital Forensik: Kebutuhan Talenta dan Jalur Sertifikasi*. Xynexis. https://xynexis.com/karier-di-dunia-digital-forensik/

Zellers, K. (2024). Hacked! North Korea's Billion-Dollar Crypto Heisting Scheme. *Penn State Journal of Law & International Affairs*, *12*(2), 10.