IJFS International Journal of Financial Systems

International Journal of Financial Systems
Volume 2, Number 2 (2024)
July-December 2024
Page : 349-378
P-ISSN : 3025-8480
E-ISSN : 3025-8537
DOI : https://doi.org/10.61459/ijfs.v2i2.75

Article History
Received : 21 October 2024
Revised : 06 December 2024
Accepted : 24 December 2024
Available Online : 31 December 2024

REGTECH ON CRYPTO FINTECH: WHAT NEEDS TO BE DONE AND ITS IMPLICATIONS FOR THE INDONESIAN ANTI-MONEY LAUNDERING MECHANISM

Kharisma Fatmalina Fajri[1],
Bima Rafly Fachrezzi[2],
Bagja Kurniawan[3]

ABSTRACT

Crypto laundering has become a significant threat in Indonesia since 2015, particularly through digital payment systems. Despite efforts to combat this threat using Regulatory Technology (RegTech), the outcomes have been largely ineffective. This study expands on previous research exploring the causes of RegTech's ineffectiveness and seeks to provide policy recommendations based on RegTech provider perspectives, for Indonesian regulators to enhance crypto laundering mitigation through RegTech. The research employed an exploratory-inductive methodology, utilising primary data from semi-structured interviews with AML operating system specialists. The data were transcribed and thematically analysed using NVivo software. The findings reveal six key themes for improving RegTech effectiveness: (1) AML mechanisms tailored to various sizes of Crypto FinTechs; (2) Access to PEP data by RegTech providers; (3) Clear classification of RegTech; (4) Strengthened collaboration between regulators and RegTech providers; (5) Regulator-led education initiatives for Crypto FinTechs; and (6) The establishment and enforcement of sanctions. These insights hold significant implications for regulatory policies aimed at preventing crypto laundering through RegTech and contribute to the application of Rational Choice and Butterfly Effect theories in understanding crypto laundering as a criminal phenomenon.

Keywords :
Indonesia, RegTech, FinTech Crypto, Crypto Laundering

JEL Classification : L24, L86, M48, Z18

[1]Universitas Islam Indonesia,
[2]Universitas Internasional Semen Indonesia,
[3]Dinas Pendidikan Provinsi Jawa Barat
*Corresponding Author: kharismaffajri@gmail.com

I. Introduction

Higher levels of economic freedom in a country are positively correlated with greater access to information and technology (Gwartney et al., 1999). This environment fosters continuous collaboration with various stakeholders. A notable example of this phenomenon is the increasing adoption of digital currencies, which offer faster, more flexible, and innovative payment methods, as well as new approaches to financing goods and services (Chuen, 2015). Cryptocurrency is a digital or virtual asset that employs encryption technology to secure transactions and manage ownership changes. It relies on blockchain or distributed ledger technologies, which provide the foundation for decentralisation and immutability (Wronka, 2024). The cryptographic nature of cryptocurrencies ensures exceptional security and trust, eliminating the need for traditional intermediaries like banks or financial institutions. Consequently, these tokens give investors a novel investment opportunity (Alaassar et al., 2023). Although transactions can be conducted with external agents and are generally governed by decentralised mechanisms, they do not always originate from open-source software, and there is often no legal entity held accountable for these activities.

By eliminating the need for intermediaries, cryptocurrency technology raises significant concerns for governments due to its potential to facilitate criminal activities (Chuen, 2015). One major concern is money laundering, a risk that gained prominence following the shutdown of Liberty Reserve, a private and centralised digital currency, over money laundering allegations (BBC News, 2013). Perpetrators of money laundering increasingly exploit the internet to conduct cyber-laundering, using digital payments and cryptocurrencies to evade detection by law enforcement (Indonesian Financial Transaction Reports and Analysis Center, 2021; (Wronka, 2022; Wronka, 2022). The challenge in detecting these activities is exacerbated by the use of multiple currencies, particularly cryptocurrencies that are user-friendly, relatively anonymous, difficult to trace, and often operate outside legal and regulatory frameworks (Leuprecht et al., 2022; van Wegberg et al., 2018). The difficulty in combating money laundering involving cryptocurrencies or their

integration with fiat currencies stems from inherent weaknesses in national and international regulatory systems, which have yet to prevent transnational money laundering activities effectively (Mugarura & Ssali, 2020; Pavlidis, 2020).

In exploring the behaviour of money launderers and strategies to combat it, Gilmour (2016) employed the Rational Choice Theory, initially proposed by (Hoomans, 1961). Gilmour (2016) argued that rational choice theory emphasises the explanation of crime at the individual level, particularly at the actual crime scene. This theory facilitates an understanding of the individuals involved, their interpersonal interactions, and their decision-making processes. As a crime prevention tool, Rational Choice Theory further elucidates how potential offenders rarely choose targets at random but instead engage in careful deliberation regarding whether to commit a particular offense. By analysing the rational decisions made by criminals involved in money laundering, Rational Choice Theory uncovers the relationship between everyday circumstances and explicitly driven activities. Therefore, applying Rational Choice Theory to money laundering reveals that the decision-making processes of perpetrators are diverse yet rational.

Indonesia, cryptocurrency and crypto assets are classified as commodities eligible for trading on the Futures Exchange (Jakfar, 2022), yet they are not recognised as legal tender due to the lack of regulation by the local monetary authority or central bank (Chen, 2018). Since 2015, virtual currencies, particularly in online black market transactions, have been identified as emerging threats in money laundering (TPPU) activities, often linked to tax evasion and online gambling, with a medium level of TPPU risk. Under Indonesian criminal law, these TPPU activities are deemed criminal offenses, subjecting both perpetrators and their virtual assets to prosecution (Utami, 2021). This situation presents a challenge for regulators who must balance minimising associated risks while fostering an environment conducive to digital innovation (Chuen, 2015). Although this phenomenon might appear less significant compared to widespread corruption in Indonesia, the Butterfly Effect Theory—first proposed by Lorenz (1963) and later expanded in economic contexts by Zhang (2021)

suggested that even small actions can lead to substantial consequences. Therefore, even seemingly minor crimes could potentially undermine the government's efforts in development and economic growth.

In response to the growing concern of money laundering, the Financial Action Task Force (FATF) has recommended that member countries ensure the registration of virtual asset service providers with local monetary authorities and enforce effective anti-money laundering (AML) systems to mitigate associated risks (FATF, 2022). Implementing digital automation systems through regulatory technology (RegTech) has emerged as a particularly effective strategy for preventing money laundering involving virtual assets and currencies, a solution increasingly recognised in jurisdictions like Indonesia (Teichmann et al., 2022)

RegTech, in its latest iteration (RegTech 3.0), shifts focus from 'Know Your Customer' (KYC) to 'Know Your Data' (KYD) (Umalkar, 2021) through the application of data analytics to anticipate potential risks (Teichmann et al., 2022). RegTech aids organisations in preventing money laundering by controlling and analysing transactions and verifying identities quickly and accurately (Zabelina et al., 2018). Recent advancements in RegTech that have proven effective for such control and analysis include machine learning (Ruiz & Angelis, 2021), artificial intelligence, and cloud computing (Kurum, 2020).

Previous research has investigated various facets of crypto laundering (Akartuna et al., 2022; Albrecht et al., 2019; Dyntu & Dykyi, 2019; Leuprecht et al., 2022; van Wegberg et al., 2018; Wronka, 2022) and the application of Regulatory Technology (RegTech) (Anagnostopoulos, 2018; Kurum, 2020; Meiryani et al., 2022; Naheem, 2018; Utami & Septivani, 2022; Utami & Septivani, 2022). However, the only study specifically addressing the use of RegTech to prevent crypto laundering was conducted by Ruiz and Angelis (2021) by examining machine learning in preventing crypto laundering and showing the results that machine learning can prevent crypto laundering but the applications of decision making in machine learning still needs to be optimised. In Indonesia, existing research has assessed the effectiveness of RegTech in combating money laundering through

quantitative approaches ((Anagnostopoulos, 2018; Kurum, 2020; Meiryani et al., 2022; Naheem, 2018; Utami & Septivani, 2022; Utami & Septivani, 2022; Meiryani et al., 2022), but it did not show significant results. There remains significant gaps in research focusing on RegTech-based crypto laundering prevention and providing policy recommendations through thematic analysis. This study aims to fill this gap by offering policy recommendations to the Indonesian regulator for preventing crypto laundering based on author's own work on previous study about the causes of RegTech ineffectiveness in this context. Additionally, it provides comprehensive findings on the improvement recommendations in line with the RegTech ineffectiveness in preventing crypto laundering, presenting a holistic view of the issue.

II. Literature Review

A. Rational Choice Theory

Rational Choice Theory suggests that criminals commit crimes because these actions are perceived as the most effective way to achieve their desired goals, such as financial gain, material possessions, prestige, sexual gratification, or power over others (Cornish & Clarke, 2002). According to this theory, criminal activities and decision-making processes are instrumental behaviours aimed at obtaining these benefits. Criminals evaluate whether to commit a crime by weighing the effort required, the potential rewards, and the associated costs of various actions. While these decision-making processes might appear straightforward, they reflect a level of rationality, though it is constrained by limitations in time, ability, and access to relevant information (Cornish & Clarke, 2016).

When applied to money laundering, Rational Choice Theory significantly supports the investigative process. It helps investigators understand the criminal methodologies used and offers a comprehensive view of the money laundering environment. Like other organised criminal activities, money laundering is complex and interconnected, making it vulnerable to more thorough investigation if properly understood. By employing this rational decomposition approach, investigators can

uncover the criminal dimensions of money laundering that may not be immediately evident during the investigation of the underlying crime.

Gilmour (2016) applied the Rational Choice Theory to argue that money laundering can be understood as a process of risk diversification, wherein individuals involved in laundering money make decisions based on a rational evaluation of their circumstances and preferences. According to this theory, money launderers engage in strategic decision-making aimed at mitigating risk and optimising their outcomes. They assess various factors such as the potential rewards, the risks of detection, and the costs associated with different laundering methods.

Gilmour's application of Rational Choice Theory highlights that money laundering, unlike some forms of crime that may stem from emotional responses or opportunistic behaviour, involves a deliberate and reasoned approach. This rationality in decision-making reflects a broader pattern observed in organised criminal activities, where individuals and groups engage in criminal behaviour as a strategic choice rather than as a result of irrational impulses. By framing money laundering within the context of Rational Choice Theory, Gilmour provides valuable insights into the methodologies employed by money launderers and the factors influencing their decisions. This perspective underscores the importance of understanding the rational processes behind money laundering, which can inform more effective investigative and regulatory strategies. It suggests that, when money laundering is scrutinised through this rational lens, it becomes possible to uncover underlying patterns and methodologies that might not be immediately apparent during investigations of the underlying predicate crimes.

B. Butterfly Effect Theory

In chaos theory, the 'butterfly effect' illustrates how small changes, such as the flapping of a butterfly's wings, can lead to significant alterations in atmospheric conditions, potentially changing the path of a tornado (Lorenz, 1963). Hardman (2021) extended this concept to money laundering, arguing that even minor instances can have far-reaching

consequences. This theory is particularly relevant for those combating financial crime, as it highlights how localised money laundering activities can escalate into global issues. While the nature of financial crime remains fundamentally the same, its impact has become more extensive. Money laundering and corruption in one part of the world can rapidly influence criminal activities elsewhere. For instance, sophisticated Ponzi schemes now operate across borders and time zones, affecting millions globally. Understanding the butterfly effect emphasises the importance of addressing even small-scale financial crimes, as they can have substantial and widespread repercussions.

While money laundering may not directly impede economic growth, as economies can continue to grow despite its presence, it often obstructs the equitable distribution of that growth. Hardman (2021) employed the Butterfly Effect to illustrate the significant threat posed by money laundering. According to Hardman, even minor instances of money laundering can escalate into substantial threats, affecting overall economic stability. This escalation underscores the need for comprehensive anti-money laundering legislation. By highlighting the potential for money laundering to grow and have widespread economic repercussions, Hardman argues for the implementation of robust legal frameworks. Such frameworks are crucial for mitigating the impacts of money laundering and ensuring that economic growth is both sustainable and fairly distributed

C. Crypto Laundering

Money laundering involving cryptocurrencies typically follows the conventional three-stage process: placement, layering, and integration. During the placement stage, the initial tracking of financial transactions occurs, and cryptocurrencies are often favoured due to their anonymity and challenges in identification (Albrecht et al., 2019; Leuprecht et al., 2022). The layering stage involves moving funds across jurisdictions through trading, investment, or exchanging cryptocurrencies with other digital assets, leveraging their virtual and stateless nature (Leuprecht et al., 2022). Finally, in the integration stage, money launderers convert

cryptocurrencies into fiat currencies to legitimise their assets (Leuprecht et al., 2022; Albrecht et al., 2019). This process is visually represented in Figure 1, which illustrates the role of cryptocurrencies in each stage of money laundering (Leuprecht et al., 2022).

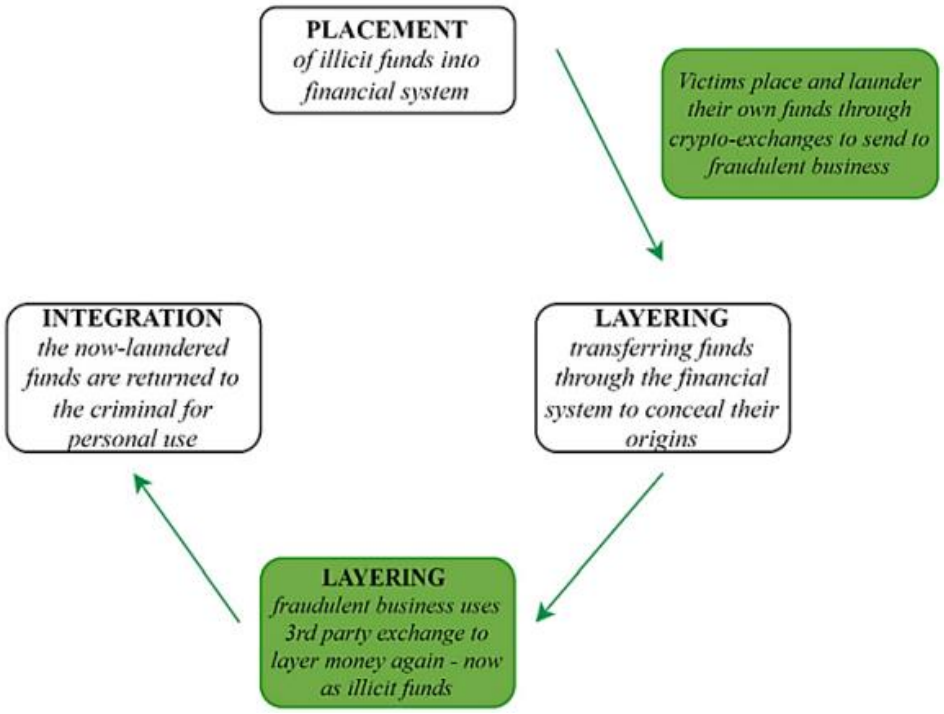

Figure 1. Money Laundering Scheme through Cryptocurrencies
Source: Leuprecht et al. (2022)

D. Regulatory Technology

Regulatory Technology (RegTech) refers to information technology solutions designed to help organisations meet legal compliance requirements by integrating trade, tax, and financial regulatory processes in a reliable, secure, and cost-effective manner (Zabelina et al., 2018). RegTech aims to enhance organisational performance by improving both efficiency and effectiveness (Anagnostopoulos, 2018). In the context of combating money laundering involving virtual currencies, RegTech is particularly valuable. It strengthens the capabilities of institutions and regulators by optimising risk mapping and facilitating thorough investigations into financial systems through advanced data analysis and information exchange (Kurum, 2020; Zabelina et al., 2018)

Table 1. The Role of RegTech in Preventing Crypto Laundering

Crypto Laundering Prevention	Objective	The Role of RegTech	Reference
Risk Assessment	Identifying and improving understanding of ML risks in the organisation	Digitalisation of surveillance systems to map potential risks	Juntunen & Teittinen (2022); Zabelina et al. (2018)
Electronic Know Your Customer (eKYC)	Obtain information about customers before starting a collaboration	Digitisation of information collection to improve the accuracy and reliability of the information obtained	Juntunen & Teittinen (2022); Meiryani et al. (2022)
Transaction Monitoring	Monitor every transaction made by customers	Identification and prediction of suspicious financial transactions	Akartuna et al. (2022); Meiryani et al. (2022)
Cost and Time Efficiencies	-	Accelerate processes and reduce ML prevention costs	Meiryani et al. (2022)

Source: Authors

RegTech is evolving rapidly and is categorised into three distinct phases (KPMG, 2018): (1) RegTech 1.0, which emerged in the 1990s to 2000s prior to the global financial crisis of 2008, with a focus on risk assessment; (2) RegTech 2.0, which began in the 2010s and emphasised 'Know Your Customer' (KYC) for anti-money laundering (AML) compliance; and (3) RegTech 3.0, which commenced in the late 2010s and centres on 'Know Your Data' (KYD) in financial crime compliance (FCC)

The data analysis process and the rapid, accurate exchange of information in RegTech are significantly enhanced by big data and cloud technology, which facilitate the collection and storage of vast volumes of unstructured data. RegTech also supports organisations by automating the reporting and detection of suspicious transactions (Zabelina et al., 2018). Its application is crucial for implementing measures to prevent money laundering and crypto laundering, as detailed in Table 1.

E. Indonesia's RegTech-based Anti-Money Laundering Mechanism Landscape

Indonesia has introduced several regulations aimed at integrating RegTech to combat money laundering, especially in the realm of cryptocurrencies. The country's approach to anti-money laundering emphasise the use of RegTech tools to enhance compliance through risk assessment, electronic know your customer (eKYC) process, and transaction monitoring. The key elements of the RegTech-based AML mechanism, along with the supporting Indonesian regulations are illustrated in Figure 2.

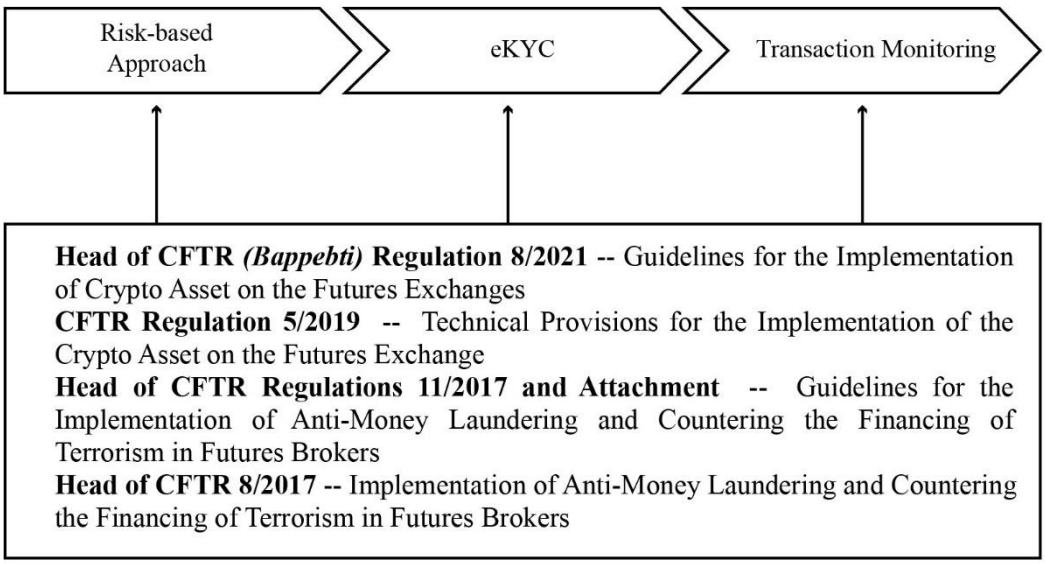

Figure 2. Key Components and Regulatory Frameworks of Indonesia's RegTech-based AML Mechanism
Source: Fajri & Urumsah (2024)

III. Data and Method

A. Research Design

The previous researches had limitations in the method applied, so this research applied an exploratory qualitative approach to obtain, process, and analyse data to explore the solutions in enhancing the use of RegTech on crypto FinTech based on RegTech provider perspectives. The qualitative approach helps researchers to answer complex questions that begin with the question words “how” and “why” (Hamilton & Finley, 2020). The qualitative approach relies heavily on reality reconstruction to answer the research questions (Saunders et al., 2012), so this research used an approach in form of semi-structured interviews with individuals. According to Hamilton & Finley (2020), qualitative research with interview, focus group, observation, and ethnography approaches is the media with the best credibility in understanding the phenomena thought by data sources, and has implications for the ease of researchers to carry out a reality reconstruction (Khalid, 2009). The researchers act as research instrument in a qualitative research (Patton, 2003), where all of the research process are mediated and interpreted by the researchers (Khalid, 2009). The qualitative approach adopted in this study allowed interview participants to share their knowledge, experiences, and perspectives, as they are considered critical participants with interests linked to the phenomenon under study (Gaskell, 2000).

B. Data Collection

The subjects in this study were individuals selected using purposive sampling technique. Individuals or interview participants represent RegTech providers with anti-money laundering operating system competencies, therefore the researchers considered that all the participants have sufficient knowledge and experience regarding the use of RegTech on crypto FinTech. Data collection was divided into two interview sessions. The first session consisted of one participant representing an international RegTech provider and was conducted via Zoom conference video application between June and July 2023. Since the lockdowns due to the COVID-19 pandemic, researchers have begun to

utilise video technology—such as: WhatsApp, Skype, Zoom, Google Meet—to conduct meetings or collect interview data (Molinari & de Villiers, 2021). The second session consisted of two participants representing national RegTech provider and was conducted offline between July and August 2023. Table 2 presents the demographic of the participants.

Table 2. Demographic Details of the Participants

Initials	Gender	Age	Competencies and Expertise	Types of RegTech
P1	Male	31-35	AML Operating System	International RegTech
P2	Male	26-30	AML Operating System	National RegTech
P3	Female	21-25	AML Operating System	National RegTech

Source: Authors

In some cases, a small sample size of data may lead to the debilitating problems for other researchers, particularly those applying assumptions of the quantitative paradigms. In contrast, qualitative research emphasises the concept of alignment, focusing on the overall congruence between what researchers have done and how they have reported it, rather than adhering to specific notion of rigour tied to particular traditions (Clarke et al., 2024). On the other hand, the ability to achieve congruence effectively depends on a researcher's grasp of both methods and theory (Yardley, 2024).

Furthermore, the researchers used video recordings for the first interview session and audio recordings for the second interview session—based on the participant's consent—to avoid researcher bias and ensure the accuracy of the data obtained. Finally, the researchers transcribed the interviews directly from the original recordings without making any changes, except for the sections the participants explicitly prohibited.

C. Data Analysis

This exploratory study adopted a qualitative data analysis approach, following Braun and Clarke's six stages of thematic analysis. Thematic analysis is a part of phenomenology (Vaismoradi et al., 2013) that focuses on finding and creating themes from the data set to answer the research questions (Sampat et al., 2023). The interview transcripts were exported into NVivo qualitative analysis data software, which was used for thematic analysis (Sampat et al., 2023). This thematic analysis applied the coding techniques referred to Social Change UK (2018) and follows a similar approach by Sampat et al. (2023), which is as follows:

1. Read and understood the entire data set without applying coding;
2. Identified key themes by applying open/initial coding;
3. Reviewed, organised, and regrouped similar themes by applying focused coding;
4. Revised the labelling of the themes in the coding results;
5. Identified the relationship of significant and relevant themes by applying axial coding;
6. Checked the consistency of the data analysis results.

After the data analysis process was completed, the researchers conducted a reliability test introduced by Morse (2002) through verification strategies. This strategy refers to the mechanism used by researchers during the research process by identifying and correcting errors from each process. In this study, the researchers ensured the suitability and alignment between the research questions, literature review, and data collection and analysis with the results of policy recommendations and interpretations of research findings. The researchers also conducted a validity test which aims to ensure that the results are a representation of the actual occurrence (Saunders et al., 2012). The validity test in this study was carried out using a triangulation technique that refers to the verification of various sources using a triangulated inquiry, consisting of elements of researchers, participants, and audiences or expertise (Hancock & Algozzine, 2006). The researchers disclosed the interview transcripts and results to the participants to ensure the truth of the researcher's findings and interpretations. The interview transcripts which were not permitted to

be known by the public were not discussed in this research. Furthermore, the researchers discussed the research findings and interpretations with two experts in forensic accounting to obtain expert reviews and a potential overview of the audience's perspective.

IV. Result and Discussion

These recommendations are based on author's own work on previous study about the causes of RegTech ineffectiveness that linked to the key stakeholders, which is shown in Figure 3.

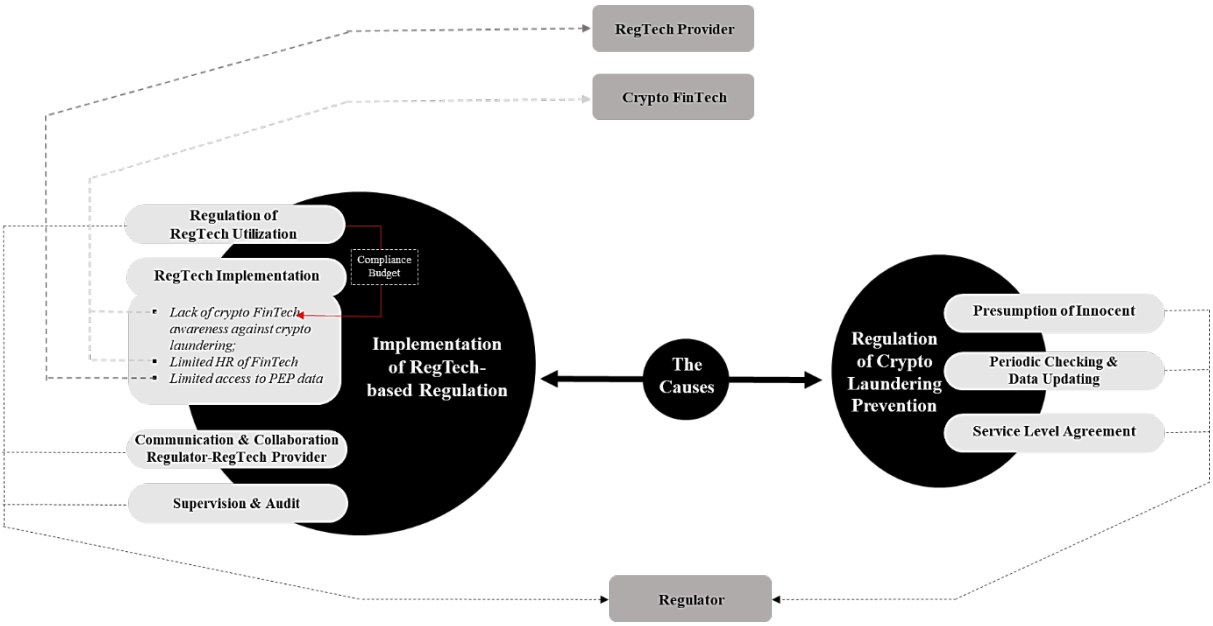

Figure 3. The Causal Factors and Key Stakeholders
Source: Author's Own Work

Furthermore, based on the results of data analysis using thematic analysis and the application of open/initial and focused coding, there are several recommendations for improvement that can be used to enhance RegTech effectiveness on crypto FinTech. Also, we applied the axial coding to identify the relationship between the causal factors with the improvement recommendations. The results of the analysis are shown in Table 3.

Table 3. Causes, Improvement Recommendations, and Implications

Causes	Improvement Recommendations	Implications
Communication and collaboration	Regulator collaboration with local RegTech providers	Standardised Vendor Due Diligence (VDD) and RegTech
RegTech regulation	RegTech classification	
Supervision and audit	Determination and provision of sanction or penalty	Supporting FATF member criteria fulfillment
RegTech Implementation	Regulator education to crypto FinTech	FinTech crypto awareness
Regulation of crypto laundering prevention on crypto FinTech	PEP data access by RegTech provider	Optimisation of data absorption
	FinTech AML mechanism at all sizes	Risk assurance and management

Source: Authors, Processed

A. Crypto FinTech AML Mechanism at All Size

This improvement recommendation is based on the causes of RegTech ineffectiveness, namely there are fundamental issues that have not been regulated in the crypto laundering prevention mechanism, causing the AML mechanism to not be implemented thoroughly by all types and size crypto FinTech. According to P2, every type and size of crypto FinTech is required to have AML mechanism because the risk of crypto laundering exist in all types and sizes of FinTech, not excluding the crypto FinTech that are still growing or small size FinTech. P2 also mentioned in the interview:

> *"Yes, they must have the procedure, and have the screening. So, when audited by regulator "Where is the screening process?" it exists, the KYC process is carried out, or for transaction monitoring "Let's see where is the transaction monitoring?", there is also in the history that*

transaction monitoring is carried out. Then also "I want to see the history of the term risk assessment", for example, if the regulator says something like that, they have evidence that they do its mechanism." (P2)

"... usually investor, especially foreign investors, have more concern in the AML. So, in addition to protecting the financial service institution from the risk of sanctions, there is also a reputational risk there." (P2)

The AML mechanism referred to in this improvement recommendation encompasses all processes, from the screening process to system-based transaction monitoring. This finding is supported by Fajri & Urumsah (2024), who highlight that the regulations governing the AML mechanism lack detailed explanations about its implementation, particularly in the context of system-based transaction monitoring. The regulations merely require organisations to apply blockchain analytic tools without specifying the types or features of such tools to be applied.

With the implementation of this improvement recommendation, it is expected to have an impact on improving the risk management applied by crypto FinTech and can provide risk assurance to regulators and investors of crypto FinTech developers, especially sanction risk and reputation risk. Risk management and assurance need to be emphasized to minimise the risk of crypto laundering carried out through the interaction between virtual systems and system in the real sector that are currently used by the majority of perpetrators (Meiryani, 2023). It is appropriate for regulators to develop system-based AML policies (RegTech) with the detailed explanations of such tools to be applied for each size of crypto FinTech, because a proper RegTech can detect risks and foresee problems that could potentially threaten the different types and sizes of crypto FinTech (Sarabdeen, 2023).

B. PEP Data Access by RegTech Provider

One of the causes of RegTech ineffectiveness on crypto FinTech in Indonesia, is due to various obstacle in the implementation of RegTech

that affect the prevention on crypto laundering. The main obstacle is closely related to access to politically exposed person (PEP) data by RegTech providers. As explained on author's previous study, RegTech providers have difficulty in obtaining PEP data because access to PEP data is limited, exclusive, and relatively given by regulator only to the IT providers, not to RegTech providers. Because PEP data is closely related to RCA (relative close associate) data, one participant conveyed it in the interview:

> *"Oh, mostly from the RCA, so family members of the high risk profile are found." (P3)*

Access to PEP data is very important and needed by RegTech providers because the potential to conduct crypto laundering can come from customers with high risk profile backgrounds and close relatives of criminal offenders or profiles that have been recorded in the Indonesia's National Blacklist (*Daftar Hitam Nasional*) or international sanction list. Therefore, according to P2, open access to PEP data obtained by RegTech providers is needed to enhance the RegTech effectiveness in preventing crypto laundering. P2 also mentioned that ideally, access to PEP data should be prioritised to be given to RegTech providers when compared to crypto FinTech or IT providers. This is because the majority of crypto FinTech or IT providers do not have adequate infrastructure to absorb, connect, and integrate the data into the RegTech system.

Technically, opening access by regulators to RegTech providers can optimise the distribution and absorption of PEP and RCA data used in RegTech. However, as discussed in the author's previous study, this finding raises new issues related to data privacy (Fajri & Urumsah, 2024). Providing access has the potential to violate ethical guidelines in the use of technology that prioritises privacy (Ryan & Stahl, 2021). Therefore, it is expected that RegTech providers can apply a flexible approach in obtaining personal data information in a legitimate and verified manner. This has implications for the role of regulator as policy makers. Regulators must have data collection guidelines for RegTech providers that ensure that data collection is carried out based on the consent of prospective

customer data. Data collection regulations or policies are developed to avoid the collection of data that is excessive, not in accordance with the purpose, inaccurate, and irrelevant (Sarabdeen, 2023). Therefore, the regulations drafted by regulators must be adequate in preventing and anticipating various challenges related to data misuse.

C. RegTech Classification

This improvement recommendation is based on the discovery of several gaps in the regulation of RegTech utilisation. According to P1, in order to improve this, so as to enhance the utilization of RegTech on crypto FinTech in Indonesia, a regulation that classifies RegTech is required. The classification of RegTech can be done based on the size and scope of RegTech in implementing system-based AML mechanism. Through this regulation, RegTech providers can have a framework that can be used as a reference when implementing RegTech. Related to this, one participant said in the interview:

> *"That's why this catalog classification can do VDD, right? Now, if for example, who is right and who is not right, it is not clear." (P1)*

With those frameworks, regulators can conduct vendor due diligence (VDD) on RegTech providers. VDD conducted by regulators aims to identify and ensure that the RegTech provider has implemented system-based AML mechanism based on regulations or framework that have been prepared. Thus, every RegTech that will be implemented on crypto FinTech has been integrally standardised based on the needs of crypto FinTech and regulators.

These findings are in line with European Banking Authority (2021) which analyses the RegTech utilisation, it is stated that based on perspective of RegTech providers, the lack of regulatory alignment is an obstacle to the RegTech utilisation, so it is necessary to converge regulatory standards. In the long-term option, convergence of regulatory standards can encourage the implementation of certification in RegTech (European Banking Authority, 2021). Thus, it is important for regulators to review and adjust one regulation with another, such as adjusting the

crypto FinTech classification with the size and scope of RegTech. If the regulations are aligned and can be implemented comprehensively, then the regulators can start to conduct VDD or certification of RegTech providers.

D. Collaboration between Regulator and RegTech Provider

This improvement recommendation is based on the obstacles in the RegTech utilisation, where the communication and collaboration between regulators and RegTech Providers are relatively ineffective. Communication by regulators is not done directly to RegTech providers, but only to crypto FinTech. Meanwhile, in terms of collaboration, one participant conveyed:

> *"Well, why regulator don't take advantage of 100% local products? It can be maximised cooperation, invited to collaborate, like that. The utilisation is maximised." (P2)*

Currently, communication between regulators and RegTech providers is not conducted directly. Regulators coordinate only with crypto FinTech, which then relay the information to RegTech providers. This raises incongruent understanding in the context of regulation changed. Regulators have not optimized the role of RegTech providers in assisting the implementation of regulations to prevent crypto laundering through the use of RegTech, including RegTech providers that have become regulatory sandboxes. According to P3, support from regulators is needed to optimise the use of RegTech in preventing crypto laundering. In line with this, P2 mentioned that support from regulators to RegTech providers can be in the form of assistance for RegTech providers in order to align with the long-term goals of regulators, mediation between RegTech providers and related institutions needed by RegTech providers.

The presence of RegTech in Indonesia plays a role in implementing Industry 4.0 and contributes to strengthening the digital ecosystem. Anshari & Almunawar (2022) found that the digital ecosystem can encourage the development of the information and communication

technology industry. So, it is important for regulators to be able to encourage the development of digital ecosystem and collaboration between interested parties in the digital ecosystem (virtual asset exchange), both parties from the public sector and the private sector because the adoption of Industry 4.0 in Indonesia is mostly carried out by the private sector (Anshari, 2020). Collaboration is an important element in the successful development of finance-related technologies (Utami & Ekaputra, 2021). This integrated communication and collaboration is expected to strengthen and facilitate regulators in applying vendor due diligence (VDD) to RegTech providers, so that the RegTech implemented is standardised and meets the needs of regulator and crypto FinTech.

E. Regulator Education to Crypto FinTech

This recommendation is based on the causes on the RegTech ineffectiveness, where there are several obstacles in the implementation of RegTech faced by RegTech providers. As the author's previous study, the obstacles are in the supervision and audit that should be carried out by regulators and RegTech implementation depend on the risk appetite and perception, and the competence of human resources from crypto FinTech. Meanwhile, in terms of supervision and audit, regulators relatively only focus on large FinTechs. However, in reality, all types and sizes of crypto FinTech have the potential to be placed for crypto laundering. To address this, one participant said in the interview:

> *"... also education from regulator, because for small to medium size FinTechs, from our cases, they usually don't understand AML." (P3)*

According to the study by Fajri & Urumsah (2024), education and training for crypto FinTech have not been incorporated into the regulation for preventing crypto laundering. Therefore, the active role of regulators is essential. Providing education to crypto FinTech human resources, particularly in small to medium-sized FinTech is part of the regulator's responsibility to ensure the successful implementation of RegTech as a technology that supports compliance function.

The suggestion for improvement is in line with the findings of Anshari & Almunawar (2022) which states that in the adoption of Industry 4.0, adequate HR knowledge and management capabilities play an important role in supporting the readiness of digital ecosystem in Indonesia. When entering Industry 4.0, organisations have fears in resource management, including human resources (Anshari & Almunawar, 2022). So, in utilising RegTech, regulators need to provide an educational platform for HR's crypto FinTech to form them to understand the impact of crypto laundering and can optimise the use of RegTech in preventing crypto laundering. The main focus of education can be related to system-based crypto laundering prevention mechanism, starting from the potential and impact of crypto laundering, the urgency of utilizing RegTech, and to the competencies that must be possessed by HR's crypto FinTech. Through this education, it is expected to increase crypto FinTech's awareness of the potential and impact of crypto laundering, and system-based crypto laundering prevention (RegTech).

F. Determination and Provision of Sanction

These improvement recommendations are based on the lacks in RegTech regulations, as well as lacks in the supervision and audit over crypto FinTech. According to P2, to emphasise that the regulations have been established must be obeyed and carried out, also the supervision and audit that carried out by regulator are in line with the objectives, the regulator needs to determine and impose sanctions on crypto FinTech, if the FinTech do not fulfill the function of compliance with established crypto laundering prevention regulations. P2 also mentioned in the interview:

> *"Just give clear sanctions, administrative sanctions, sanctions that are even strict, give clear and start implementing the sanctions, so that there is implication from small things ..." (P2)*

> *"... the sanction must be emphasised, then also mention the industries that are required, expanded again ..." (P2)*

This determination and provision of sanction also emphasised that the applicable regulation is a necessity and urgent. Sanctioning of crypto FinTech can be tiered, ranging from the administrative sanctions to more binding sanctions.

According to Teichmann & Wittmann (2023), a secure AML mechanism should encourage smoothness and assertiveness in the application of sanctions related to the compliance function. This is a reflection for regulators, it is possible that the AML mechanism in virtual asset (crypto) trading in Indonesia in not adequate and optimal. So, it is important for regulators to test and review the resilience and adequacy of system-based AML mechanism in overcoming problems that may arise in the RegTech utilisation, including the compliance of crypto FinTech in utilising RegTech. With the determination and provision of strict sanctions of crypto FinTech, it is expected to encourage the readiness of financial services institutions in implementing system-based AML mechanism, so as to support the strengthening of Indonesia as a member country of the FATF (Financial Action Task Force) with full membership status.

V. Conclusion

This study offers qualitative insights into the improvement recommendations for enhancing RegTech effectiveness in preventing crypto laundering, drawing on the cause findings of previous study from the perspective of RegTech provider. These insights provide significant policy recommendations, emphasising the importance of the regulator's role in drafting and enforcing AML mechanism on crypto FinTech.

The findings reveal that improving communication, collaboration, and data access between regulators and RegTech providers is essential. Additionally, policies promoting better education for crypto FinTech, along with more defined penalties for non-compliance, can further strengthen AML efforts. These recommendations are designed to optimise RegTech effectiveness, ensuring it serves as a robust tool in combating financial crime.

However, we acknowledge several limitations that suggest avenues for future research. First, the qualitative approach may introduce a degree of subjectivity, as the data were collected exclusively from the perspectives of RegTech providers. The study's scope was limited by the inability to include insights from FinTech crypto users of RegTech. Future research could address this by incorporating the FinTech crypto perspective, offering a more comprehensive understanding of the improvements that can be included to AML mechanism on crypto FinTech. Second, this study primarily focused on economic and legal aspects, leaving political factors unexplored. Future research could integrate economic, legal, and political dimensions, potentially leading to a more nuanced and expansive set of findings.

VI. Policy Recommendations

This study provides policy recommendations for improving and enhancing anti-money laundering in crypto FinTech. As found and discussed in this study, regulators play an important role in AML mechanisms.

First, we recommend regulators to develop AML mechanisms for all types and sizes of FinTech that are aligned with the RegTech category that should be implemented. For example, in a small FinTech, the RegTech used is a RegTech with the same size and scope, so as to avoid the refusal of FinTech to use RegTech because the cost is too high.

Second, the applicable AML mechanism should be able to cover all elements that play a role in the prevention of crypto laundering, and anticipate and predict various events that may occur in the future. First, the Indonesia’s AML mechanism does not regulate the education and training of FinTech human resources. The AML mechanism only regulates the requirements in the selection of HR through the KYE (know your employee) process carried out before entering a work engagement, so the findings of the recommendations in this study encourage regulators to provide education and training to FinTech HR. For example, in improving the AML mechanism for crypto FinTech, Indonesia can reflect on the AML

mechanism applicable in the UK, where education and training of human resources directly related to the prevention of crypto laundering is part of the crypto laundering prevention mechanism. Second, the findings and discussions regarding the opening of PEP data access to RegTech providers encourage regulators to develop detailed personal data acquisition and use policies and become an integral part of the AML mechanism that must be complied with by crypto FinTech.

Third, the enforcement of regulations along with sanctions given to crypto FinTechs (if violated) must be a written part of the AML mechanism. This aims to encourage the compliance function of crypto FinTechs and emphasise the role of regulators as regulatory enforcers.

REFERENCES

Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting and Social Change*, *179*(2021), 1–30. https://doi.org/10.1016/j.techfore.2022.121632

Alaassar, A., Mention, A.-L., & Aas, T. H. (2023). Facilitating innovation in FinTech: a review and research agenda. *Review of Managerial Science*, *17*(1), 33–66. https://doi.org/10.1007/s11846-022-00531-x

Albrecht, C. Duffin, K. M. K., Hawkins, S., & Rocha, V. M. M (2019). The Use of Cryptocurrencies in the Money Laundering Process. *Journal of Money Laundering Control*, *22*(2), 210–216. https://doi.org/10.1108/JMLC-12-2017-0074

Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business*, *100*, 7–25. https://doi.org/10.1016/j.jeconbus.2018.07.003

Anshari, M. (2020). Workforce Mapping of Fourth Industrial Revolution: Optimization to Identity. *Journal of Physics: Conference Series*, *1477*(7). https://doi.org/10.1088/1742-6596/1477/7/072023

Anshari, M., & Almunawar, M. N. (2022). Adopting open innovation for SMEs and industrial revolution 4.0. *Journal of Science and Technology Policy Management*, *13*(2), 405–427. https://doi.org/10.1108/JSTPM-03-2020-0061

Chen, L. M. (2018). School-based anti-bullying strategies in Taiwan and their effects. *Studies in Educational Evaluation*, *59*, 218–223. https://doi.org/10.1016/j.stueduc.2018.09.004

Chuen, D. L. K. (2015). Bitcoin, Innovation, Financial Instruments, and Big Data. In *HANDBOOK OF DIGITAL CURRENCY*. Elsevier.

Clarke, V., Braun, V., Adams, J., Callaghan, J. E. M., LaMarre, A., & Semlyen, J. (2024). " Being Really Confidently Wrong ": Qualitative Researchers ' Experiences of Methodologically Incongruent Peer Review Feedback. *Qualitative Psychology*, *Advance Online Publication*. https://doi.org/https://dx.doi.org/10.1037/qup0000322

Cornish, D., & Clarke, R. V. (2002). *Analyzing organized crimes. In: Piquero, Alexis, Tibbetts, Stephen (Eds.), Rational Choice and Criminal*

Behaviour. Routledge.

Cornish, D., & Clarke, R. V. (2016). *The Reasoning Criminal* (D. B. Cornish & R. V. Clarke (eds.)). Routledge. https://doi.org/10.4324/9781315134482

Dyntu, V., & Dykyi, O. (2019). Cryptocurrency in the System of Money Laundering. *Baltic Journal of Economic Studies*, *4*(5), 75–81. https://doi.org/10.30525/2256-0742/2018-4-5-75-81

European Banking Authority. (2021). *Analysis of RegTech in the EU Financial Sector* (Issue June). Retrieved from https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1015484/EBA analysis of RegTech in the EU financial sector.pdf.

Fajri, K. F., & Urumsah, D. (2024). Crypto Laundering Prevention in Indonesia: The Role of Regulatory Technology and Financial Intelligence Unit. *Journal of Accounting and Investment*, *25*(3). https://doi.org/10.18196/jai.v25i3.22170

FATF. (2022). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. *FATF, Paris, France*, *March*, 1–142. Retrieved from www.fatf-gafi.org/recommendations.html

Gaskell, G. (2000). *Individual and Group Interviewing. Qualitative Researching with Text, Image and Sound*. SAGE.

Gilmour, N. (2016). Preventing money laundering: a test of situational crime prevention theory. *Journal of Money Laundering Control*, *19*(4), 376–396. https://doi.org/10.1108/JMLC-10-2015-0045

Gwartney, J., Holcombe, R., & Lawson, R. (1999). Economic Freedom and the Environment for Economic Growth. *Journal of Institutionaland Theoretical Economics 155*, *155*(4), 643–663.

Hamilton, A. B., & Finley, E. P. (2020). Reprint of: Qualitative methods in implementation research: An introduction. *Psychiatry Research*, *283*(2019), 112629. https://doi.org/10.1016/j.psychres.2019.112629

Hancock, D., & Algozzine, B. (2006). *A Practical Guide for Doing Case Study Research*.

Hardman, J. (2021). The butterfly effect: Theoretical implications of an apparently minor corporate transparency proposal. *Common Law World Review*, *50*(4), 180–197. https://doi.org/10.1177/14737795211037701

Hoomans, G. (1961). *Social Behaviour: Its Elementary Forms*. Routledge and

Kegan Paul.

Indonesian Financial Transaction Reports and Analysis Center. (2021). *Penilaian Risiko Indonesia Pencucian Uang*. Pusat Pelaporan dan Analisis Transaksi Keuangan.

Jakfar, B. N. (2022). Perbandingan Hukum tentang Mata Uang Virtual sebagai Aset Terpidana Tindak Pidana Korupsi di Indonesia. *Jurnal Ilmiah Indonesia*, *7*(7), 9898–9911. Retrieved from https://www.who.int/news-room/fact-sheets/detail/autism-spectrum-disorders

Juntunen, J., & Teittinen, H. (2022). Accountability in anti-money laundering – findings from the banking sector in Finland. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-12-2021-0140

Khalid, S. N. A. (2009). Reflexivity in Qualitative Accounting Research. *Journal of Financial Reporting and Accounting*, *7*(2), 81–95. https://doi.org/10.1108/19852510980000005

KPMG. (2018). *There's a Revolution Coming: Embracing the Challenge of RegTech 3.0*. https://assets.kpmg/content/dam/kpmg/uk/pdf/2018/09/regtech-revolution-coming.pdf

Kurum, E. (2020). RegTech solutions and AML compliance: what future for financial crime? *Journal of Financial Crime*. https://doi.org/10.1108/JFC-04-2020-0051

Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-07-2022-0161

Lorenz, E. (1963). The Predictability of hydrodynamic flow. *Transactions of The N.Y Academy of Science*, *25*, 409–432.

Meiryani. (2023). Exploration of potential money laundering crimes with virtual currency facilities in Indonesia. *Journal of Money Laundering Control*, *2022*(Wcp 2022). https://doi.org/10.1108/JMLC-01-2023-0010

Meiryani, M., Soepriyanto, G., & Audrelia, J. (2022). Effectiveness of regulatory technology implementation in Indonesian banking sector to prevent money laundering and terrorist financing. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-04-2022-0059

Molinari, M., & de Villiers, C. (2021). Qualitative accounting research in the time of COVID-19 – changes, challenges and opportunities. *Pacific*

Accounting Review, *33*(5), 568–577. https://doi.org/10.1108/PAR-09-2020-0176

Morse, J. K. (2002). Verfication Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods*, *1*(2). https://doi.org/10.5862/MCE.55.7

Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, *24*(1), 10–28. https://doi.org/10.1108/JMLC-11-2019-0092

Naheem, M. A. (2018). TBML suspicious activity reports – a financial intelligence unit perspective. *Journal of Financial Crime*, *25*(3), 721–733. https://doi.org/10.1108/JFC-10-2016-0064

Patton, M. Q. (2003). Qualitative Research and Evaluation Methods (3rd ed.). In *Evaluation Journal of Australasia* (Vol. 3, Issue 2, pp. 60–61). https://doi.org/10.1177/1035719X0300300213

Pavlidis, G. (2020). International regulation of virtual assets under FATF's new standards. *Journal of Investment Compliance*, *21*(1), 1–8. https://doi.org/10.1108/joic-08-2019-0051

Ruiz, E. P., & Angelis, J. (2021). Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges. *Journal of Money Laundering Control*, *25*(4), 766–778. https://doi.org/10.1108/JMLC-09-2021-0106

Ryan, M., & Stahl, B. C. (2021). Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications. *Journal of Information, Communication and Ethics in Society*, *19*(1), 61–86. https://doi.org/10.1108/JICES-12-2019-0138

Sampat, B., Mogaji, E., & Nguyen, N. P. (2023). The dark side of FinTech in financial services: a qualitative enquiry into FinTech developers' perspective. *International Journal of Bank Marketing*. https://doi.org/10.1108/IJBM-07-2022-0328

Sarabdeen, J. (2023). Laws on regulatory technology (RegTech) in Saudi Arabia: are they adequate? *International Journal of Law and Management*. https://doi.org/10.1108/IJLMA-03-2023-0042

Saunders, M., Lewis, P., & Thornhill, A. (2012). Research methods for business students. In *International Journal of the History of Sport* (Vol. 30, Issue 1). www.pearson.com/uk

Social Change UK. (2018). *An Introductory Guide to Qualitative Research Analysis*. https://social-change.co.uk/files/Knowledge_Hub_-_qualitative_research_analysis.pdf%0Ahttps://social-change.co.uk/blog/a-brief-guide-to-qualitative-research-analysis

Teichmann, F., Boticiu, S., & Sergi, B. S. (2022). RegTech - Potential Benefits and Challenges of Businesses. *Technology in Society*. https://doi.org/10.1016/j.techsoc.2022.102150

Teichmann, & Wittmann, C. (2023). Practical considerations regarding the implementation of economic sanctions by Swiss financial service providers. *Journal of Money Laundering Control*. https://doi.org/https://doi.org/10.1108/JMLC-12-2022-0167

Umalkar, M. (2021). RegTech: An Untapped Opportunity. *Journal of Digital Banking*, *6*(1), 72–82.

Utami, A. M., & Septivani, M. D. (2022). Regulatory Technology (RegTech): The Solution to Prevent Money Laundering in Indonesia. *Telaah Bisnis*, *23*(1), 86. https://doi.org/10.35917/tb.v23i1.288

Utami, A. M., & Septivani, M. D. (2022). Solutions to money laundering prevention through Regulatory Technology (RegTech): Evidence from Islamic and conventional banks. *Jurnal Ekonomi & Keuangan Islam*, *8*(1), 17–31. https://doi.org/10.20885/jeki.vol8.iss1.art2

Utami, & Ekaputra. (2021). A paradigm shift in financial landscape: encouraging collaboration and innovation among Indonesian FinTech lending players. *Journal of Science and Technology Policy Management*, *12*(2), 309–330. https://doi.org/https://doi.org/10.1108/JSTPM-03-2020-0064

Utami, S. (2021). Tindak Pidana Pencucian Terhadap Uang Virtual Money Laundering on Virtual Money. *Al-Adl : Jurnal Hukum*, *13*(1), 1–27. https://ojs.uniska-bjm.ac.id/index.php/aldli/article/view/4224

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content Analysis and Thematic Analysis: Implications for Conducting a Qualitative Descriptive Study. *Nursing and Health Sciences*, *15*(3), 398–405. https://doi.org/10.1111/nhs.12048

van Wegberg, R., Oerlemans, J. J., & van Deventer, O. (2018). Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, *25*(2), 419–435. https://doi.org/10.1108/JFC-11-2016-0067

Wronka, C. (2022). Anti-money laundering regimes: a comparison between Germany, Switzerland and the UK with a focus on the crypto business. *Journal of Money Laundering Control*, *25*(3), 656–670. https://doi.org/10.1108/JMLC-06-2021-0060

Wronka, C. (2022). "Cyber-laundering": the change of money laundering in the digital age. *Journal of Money Laundering Control*, *25*(2), 330–344. https://doi.org/10.1108/JMLC-04-2021-0035

Wronka, C. (2022). Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*, *25*(1), 79–94. https://doi.org/10.1108/JMLC-02-2021-0017

Wronka, C. (2024). Crypto-asset regulatory landscape: a comparative analysis of the crypto-asset regulation in the UK and Germany. *Journal of Asset Management*, *25*(4), 417–426. https://doi.org/10.1057/s41260-024-00358-z

Yardley, L. (2024). *Qualitative Psychology: A Practical Guide to Research Methods* (4th ed.). SAGE Publishing.

Zabelina, Vasiliev, & Galushkin. (2018). Regulatory Technologies in the AML/CFT. *KnE Social Sciences*, *3*(2), 394. https://doi.org/10.18502/kss.v3i2.1569

Zhang, W.-B. (2021). *The Butterfly Effect in China's Economic Growth*. Springer Singapore. https://doi.org/10.1007/978-981-15-9889-0