Article Type: Literature Review

Crypto laundering prevention in Indonesia: The role of regulatory technology and financial intelligence unit

Kharisma Fatmalina Fajri* and Dekar Urumsah

Abstract

Research aims: In Indonesia, crypto laundering has become an emerging threat through digital payments since 2015. This study aims to elaborate the crypto laundering prevention through the utilization of regulatory technology (RegTech) and the role of the Financial Intelligence Unit (FIU).

Design/Methodology/Approach: The study was conducted using a qualitative content analysis approach with the support of NVivo 12. Data was sourced from secondary data in the form of law documents that have been established and published by the Commodity Futures Trading Regulatory Agency (CFTR).

Research findings: Crypto laundering prevention is implemented through Know Your Customer (KYC) and transaction monitoring based on a risk-based approach. Normatively, KYC and transaction monitoring should be implemented on RegTech-based face recognition for KYC and blockchain analytic tools for transaction monitoring. Furthermore, the findings revealed that the FIU in Indonesia is the Indonesian Transaction Report and Analysis Center (INTRAC) which has the authority to receive and conduct further analysis of transaction monitoring results. INTRAC conducts advanced analysis with a 'follow the money' approach. The existence of INTRAC's role depends on the tools, technology, and human resources that represent it.

Theoretical contribution/Originality: This study contributes to knowledge in the field of forensic accounting. The findings and discussions in this study provide valuable insights into the current contemporary accounting issues and their relationship with other disciplines.

Practitioner/Implication: This study provides insights for regulators to collaborate with various experts from information technology and environmental fields regarding developing regulations and policies to prevent crypto laundering.

Research limitation: The data used was only sourced from secondary data (regulatory documents), so the role of RegTech and FIU was only studied normatively.

Keywords: Indonesia; Crypto Laundering; Blockchain; RegTech; Financial Intelligence Unit

AFFILIATION:
Department of Accounting, Faculty of Business and Economics, Universitas Islam Indonesia, Special Region of Yogyakarta, Indonesia

***CORRESPONDENCE:**
kharismaffajri@gmail.com

DOI: 10.18196/jai.v25i3.22170

CITATION:
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), 1133-1155.

ARTICLE HISTORY
Received:
24 Apr 2024
Revised:
17 Jul 2024
03 Sep 2024
Accepted:
23 Sep 2024

JAI Website:

Introduction

Money laundering (ML) is an intangible process used to disguise the origin of profits generated through criminal activities (Gottschalk, 2010). In other words, ML means securing the proceeds of illicit funds committed by the perpetrator (Pontes et al., 2022). ML has become an important activity in financial crime (Gottschalk, 2010) because it consists of concealment

(Pickett & Pickett, 2002) and conversion process (Albrecht et al., 2012) of predicate crime, such as fraud, corruption, and theft. The proceeds of ML activities are integrated with lawful economic processes so that the perpetrators can use their 'illicit funds' legally because the purpose of ML is to transform unlawful proceeds into lawful ones (Gottschalk, 2010). With this typology and ecosystem, the nature of the anti-money laundering (AML) system must be responsive and preventive (Basel Institue of Governance, 2021) of the various ML techniques that may occur, considering human lifestyles and technological advances greatly affect the dynamics of ML activities (Wronka, 2022a).

The dynamics of ML activities are greatly affected by technological advances, digital development, and the use of the internet, which perpetrators utilize to commit ML with the latest techniques (Mugarura & Ssali, 2020) via online transactions (cyber laundering) by using digital payments and virtual currencies (cryptocurrencies). The use of virtual currencies aims to avoid and complicate detection by law enforcement officials (Wronka, 2022a; Wronka, 2022b; Mardiansyah, 2021). The difficulty of detection is due to the fact that cyber laundering uses more than one currency (multiple currencies), where the perpetrators use cryptocurrencies that are easy to use, relatively anonymous, difficult to trace, and unrestricted by laws and regulations (van Wegberg et al., 2018; Leuprecht et al., 2022). The perpetrators use cryptocurrencies in the placement and layering stages and then use fiat currencies in the integration stage (Leuprecht et al., 2022). The use of cryptocurrencies in ML activities continues to grow, with cases increasing exponentially (Dyntu & Dykyi, 2019), as of a 30% increase by 2021 (Chainalysis, 2022).

In Indonesia, crypto users and owners accounted for 15% of the population as of October 2022, which is higher than the global average of 14% of the population (Finder, 2022). Cryptocurrency and crypto assets are determined as commodities that can be traded on futures exchanges (Jakfar, 2022), but they are not legal tender because of uncontrolled by the local monetary authority (central bank) (Kementerian Keuangan RI, 2022). Virtual currency (cryptocurrency) has been known as an emerging threat to ML in Indonesia since 2015. It is used in commerce activities with accounts used on behalf of others, and e-commerce misappropriates in transactions of the proceeds of crime, unlicensed peer-to-peer lending on financial technology activities, and used in digital money network transactions on online black markets as a proceed of tax crimes and online gambling, with a medium level of ML risk (Mardiansyah, 2021).

In response to these challenges that affect the AML systems and increase threats to both regional and global economic stability, the Financial Action Task Force (FATF) gives recommendations to their member countries to ensure that virtual asset providers must be registered with local monetary authority and comply with AML systems to mitigate risks and prevent money laundering via virtual assets (FATF, 2022). The use of virtual assets in illegal activities reaches more than 37 million transactions per year (Leuprecht et al., 2022), thus generating a large amount of data. The sheer volume and proliferation of data make financial institution's compliance with AML systems and suspicious transaction reporting more costly and complicated (Teichmann et al., 2022). Therefore, the adoption of digital automation through regulatory technology (RegTech) with the latest version (RegTech 3.0) is an effective solution for preventing ML involving virtual

assets (crypto laundering) (Teichmann et al., 2022). Some of the latest technologies in RegTech have been proven to help control and analyze (Zabelina et al., 2018), such as machine learning (Singh et al., 2022; Ruiz & Angelis, 2021), artificial intelligence (Singh & Lin, 2021; Kurum, 2020), and cloud computing (Kurum, 2020). The use of RegTech in preventing crypto laundering needs to be accompanied by the Financial Intelligence Unit (FIU) as an independent institution whose role is to receive and follow up on every suspicious transaction reported by financial institutions (Lukito, 2016; Naheem, 2018). The role of FIU and financial institutions together aims to achieve good synergy in overcoming various obstacles related to ML (Lukito, 2016).

Several studies on cryptocurrency and crypto assets have been conducted (Leuprecht et al., 2022; Wronka, 2022c; Akartuna et al., 2022; Albrecht et al., 2019; Dyntu & Dykyi, 2019; van Wegberg et al., 2018), which validated that cryptocurrencies and crypto asset are used in the money laundering process, especially at the placement and layering stages. Meanwhile, studies on RegTech utilization (Utami & Septivani, 2022b; Utami & Septivani, 2022a; Meiryani et al., 2022; Kurum, 2020; Naheem, 2018; Anagnostopoulos, 2018) indicated that RegTech and its underlying technologies are becoming impactful technologies for financial institutions to fight financial crime, although some studies showed insignificant results due to various inhibiting factors. Then, the use of financial intelligence and the role of FIU have been studied (Reznik et al., 2021; Sultana, 2020; Lukito, 2016), emphasizing the importance of financial intelligence and the role of FIU in combating financial crimes and that the lack of FIU's role may accelerate the exchange of income obtained from financial crimes. A study that specifically explains the use of RegTech in preventing crypto laundering was only 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 optimized. Therefore, this study focuses on the RegTech utilization in the anti-crypto laundering system with the addition of the FIU role's discussion, which carries out the supervisory function in the anti-crypto laundering (Sultana, 2020).

For that reason, this study aims to explain the mechanism of crypto laundering prevention involving the RegTecg utilization and FIU's role in Indonesia, which is currently still developing and improving (Otoritas Jasa Keuangan, 2022). The elaboration of this study refers to the laws and regulations issued by the Commodity Futures Trading Regulatory Agency (CFTR). The analysis process begins with a theoretical elaboration of RegTech and the role of FIU in preventing crypto laundering. Furthermore, the mechanism of RegTech-based crypto laundering prevention and the role of FIU in the crypto laundering prevention mechanism is enriched with discussions of the impact of RegTech's underlying technologies on data privacy and environmental sustainability, as well as discussions on strengthening the existence of Indonesian Transaction Report and Analysis Center/INTRAC's role as FIU in Indonesia.

This study contributes to the body of knowledge in the field of forensic accounting, particularly on the topic of money laundering. The findings and discussions in this study provide valuable insights into current contemporary accounting issues, as well as their relationship with various other scientific disciplines. In addition, this study provides

practical implications for the Commodity Futures Trading Regulatory Agency and the Financial Service Authority as stakeholders. The findings of this study also provide insights into how regulators collaborate with various experts from information technology and environmental fields in developing regulations and policies to prevent crypto laundering.

Literature Review

Crypto Laundering Prevention through RegTech and Financial Intelligence Unit

Crypto assets or cryptocurrencies are virtual currencies that were first introduced by Satoshi Nakamoto in 2009 by creating bitcoin as a type of currency in cryptocurrencies (Albrecht et al., 2019). Unlike fiat currencies that are legally issued by a country, this virtual currency is not issued and not bound by a country (stateless) and is intangible by relying on blockchain as a virtual ledger to ensure the stability of the currency value (Adachi & Aoyagi, 2020). Currency value stability of the currency can be guaranteed because every cryptocurrency transaction that contains a series of codes in a virtual ledger is encrypted and verified by the blockchain (Litchfield, 2015).

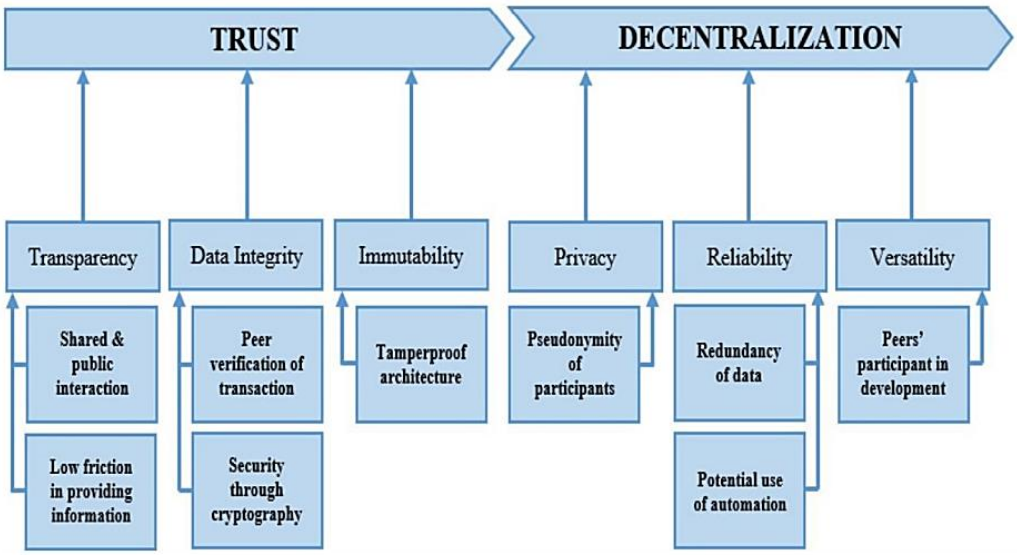


Figure 1 Characteristics of Blockchain Technology
Source: Seebacher and Schüritz (2017)

Blockchain is open public, so the transactions that are encrypted and verified are all cryptocurrency transactions with the aim of compiling a 'blockchain' and not compiling transactions belonging to each individual or organization (Albrecht et al., 2019). Each block stores a cryptographic hash (set of codes) of the previous block that compiles the chain, where the cryptographic hash also takes the data from the previous block and converts it into a compact string (Zaman et al., 2023). The string is unpredictable, so the block connection makes the chain secure and decentralized (Zaman et al., 2023), or there is no centralized server that holds transactions. Thus, each block must meet the requirements of the chain so that no transaction can replace the previous transaction

(Moore, 2018). Besides having decentralized characteristics, blockchain technology also has trust characteristics (Seebacher & Schüritz, 2017). Each characteristic has sub-attributes illustrated in Figure 1 (Seebacher & Schüritz, 2017). Meanwhile, the process of recording transactions that occur in blockchain technology to form a 'blockchain' is depicted in Figure 2 (Bylund, 2023).

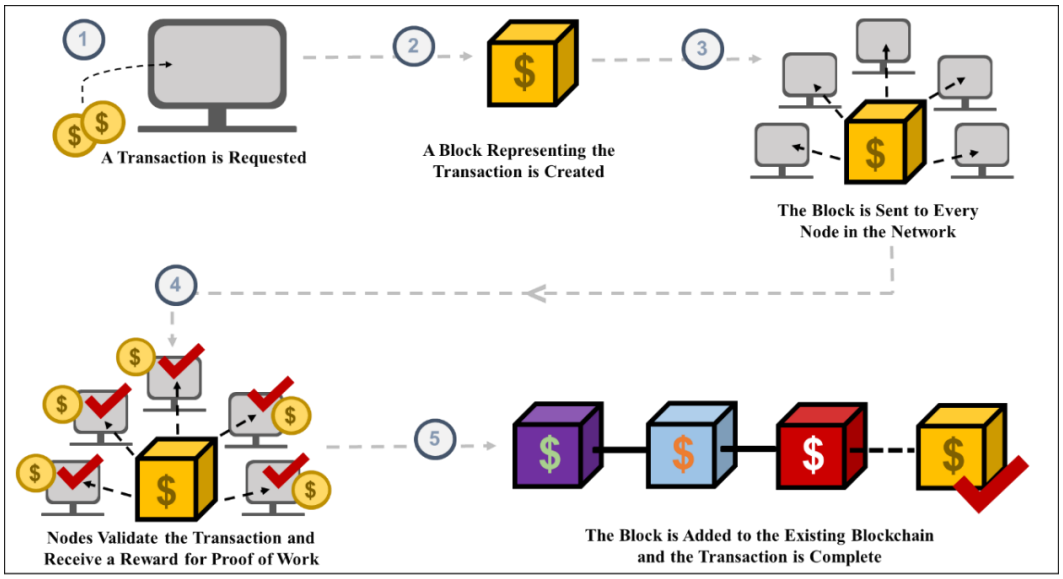


Figure 2 Transaction Recording Process in Blockchain
Source: Bylund (2023)

The fundamental differences between fiat currencies and cryptocurrencies in payment transactions (Wronka, 2022c) are presented in Table 1.

By their nature, cryptocurrencies do not require banks or other intermediary institutions to make financial transactions (Peters et al., 2015), and owners of such financial transactions are difficult to identify due to their relative anonymity (van Wegberg et al., 2018; Albrecht et al., 2019; Leuprecht et al., 2022; Al-Tawil, 2022). As a result, financial criminals started using cryptocurrencies during the ML process (Albrecht et al., 2019). Perpetrators can easily move funds from one country to another country in a network of cryptocurrencies with an internet connection only due to their stateless nature and the absence of a central governing authority (Albrecht et al., 2019). With such ease, cryptocurrencies pose a threat to the security of the global financial system (Al-Tawil, 2022). Recent data reveals that there was a 30% increase from 2020 to 2021 in the use of cryptocurrencies for ML activities in darknet markets, and this does not include ML activities through cryptocurrencies integrated with fiat currencies (Chainalysis, 2022). The use of crypto-fiat currencies integration through the conversion of fiat currencies to cryptocurrencies and vice versa is done by perpetrators to make a difficult detection (Leuprecht et al., 2022).

Table 1 The Differences between Fiat Currencies and Cryptocurrencies

	Fiat Currencies	Cryptocurrencies
Financial institution	Banks and payment institutions	No institution is involved, but crypto platforms are instead
Storage of the transactions	Central at the institute	Decentralized on the blockchain
Business Partner	Known person	Pseudonym, a known person if applicable
Customer	Identified person	Pseudonym, identified person if applicable
Storage and disposal	Banknotes and cards	Wallet with the public keys
Access to the assets	PIN/signature/cheque	Private key
Allocation of the payment	IBAN with Bank Identification Code (BIC)	Public key
Monitoring of the transactions	Accounts and payment transactions	Blockchain

Source: Wronka (2022c)

Like the conventional ML process, the ML process through cryptocurrencies also consists of three main stages: placement, layering, and integration. First, placement is a very important stage and the beginning of tracing the financial transactions (Albrecht et al., 2019). At this stage, perpetrators use cryptocurrencies that are anonymous and difficult to identify (Leuprecht et al., 2022). Perpetrators exchange fiat currencies derived from illegal activities for cryptocurrencies (Wronka, 2022c). Second, layering, perpetrators use cryptocurrencies across multiple jurisdictions through trading, investing, or exchanging coins with other types of cryptocurrencies due to their virtual and stateless nature (Leuprecht et al., 2022). This technique is commonly referred to as chaining of transactions (Wronka, 2022c). Another technique commonly used is the mixer technique, which works by combining multiple transactions and distributing them across different wallets, making it more difficult to trace transactions to the source of funds (Wronka, 2022c). Third, integration is stage to carried out by perpetrators to exchange cryptocurrencies with fiat currencies (Leuprecht et al., 2022; Albrecht et al., 2019) so that proceeds from ML can be used in the legitimate monetary cycle (Wronka, 2022c).

The crypto laundering process (Leuprecht et al., 2022) is illustrated in Figure 3.

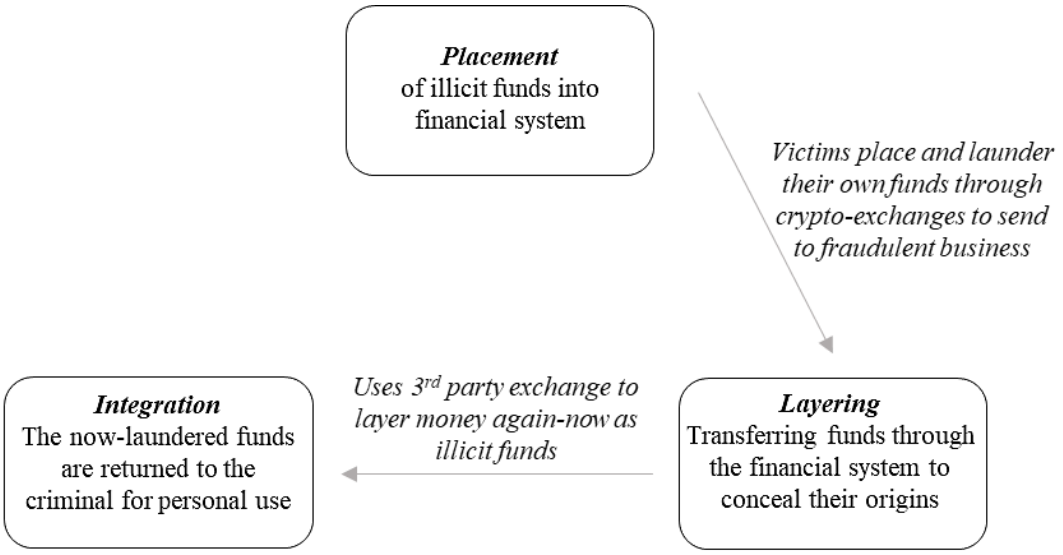


Figure 3 Crypto Laundering Process
Source: Leuprecht (2022)

In an effort to minimize the impact of crypto laundering, organizations implement and improve system-based prevention mechanisms through the application of RegTech (Ruiz & Angelis, 2021). RegTech is an information technology that can assist and support organizations in meeting compliance with legal requirements through reliable, safe, and economical solutions (Zabelina et al., 2018). RegTech aims to improve the efficiency and effectiveness of organizational performance (Anagnostopoulos, 2018). RegTech is utilized for preventing crypto laundering because it can increase the ability of institutions and regulators to fight financial crime (Kurum, 2020) by optimizing risk mapping and investigating the financial system through data analysis and information exchange (Zabelina et al., 2018). RegTech is evolving rapidly and is divided into three phases (KPMG, 2018), namely: (1) RegTech 1.0, which started in the 1990s to 2000s before the global crisis in 2008 and focused on risk assessment; (2) RegTech 2.0 started in the 2010s and focused on Know Your Customer (KYC) for AML compliance; and (3) RegTech 3.0 started in the 2019s and focused on Know Your Data (KYD) in financial crime compliance (FCC) by using data analytics to predict the risks that will occur (Teichmann et al., 2022). The process of analyzing data and exchanging information quickly and accurately in RegTech can be done because RegTech uses big data and cloud technology to collect and store large amounts of unstructured data. RegTech also helps organizations for automate reporting and detection of suspicious transactions (Zabelina et al., 2018). RegTech helps organizations in carrying out crypto laundering prevention as presented in Table 2.

Table 2 RegTech's Role in Crypto Laundering Prevention

Crypto Laundering Prevention	Objective	RegTech's Role	Reference
Risk Assessment	Identify and improve understanding of ML risks to the organization	Digitalization of surveillance system for potential risk mapping	Juntunen & Teittinen (2022); Zabelina et al. (2018)
Electronic Know Your Customer (eKYC)	Obtaining customer's information and financial record background	Digitalization of information collection to improve the accuracy and reliability of the information obtained	Juntunen & Teittinen (2022); Meiryani et al. (2022)
Transaction Monitoring	Supervise every transaction made by customers	Identification and prediction of suspicious transactions	Akartuna et al. (2022); Meiryani et al. (2022)
Cost and Time Efficiencies	-	Accelerate processes and lower ML prevention costs.	Meiryani et al. (2022)

Source: Authors (2023)

To create an integral crypto laundering prevention effort and reduce the systematic risk of crypto laundering—which can disrupt international financial and economic stability—the use of RegTech needs to be complemented by financial monitoring (Reznik et al., 2021). Financial monitoring is a part that needs to be considered because it is an integral part of financial control in the economic aspect of a country. A specific form of financial control approach is through the application of financial intelligence (Reznik et al., 2021) with the scope presented in Table 3.

Table 3 Scope of Financial Intelligence

Controller	Controlled	Controlled Object	Purpose
Institutions with financial control functions designated by the state	All types of business entities, institutions, organizations, and individuals	Legality, use, reliability, and economic efficiency of financial activities	Prevent transactions that may be related to ML activities

Source: Reznik et al. (2021)

The application of financial intelligence is carried out by an institution (controller) appointed or established by the state. The naming of the institution may vary from one country to another, but it is generally referred to as the Financial Intelligence Unit (FIU) (Reznik et al., 2021) and acts as the coordinator for AML in the country (Sultana, 2020; Naheem, 2018). The main function or internal function of the FIU is to collect, analyze, and disseminate reports on entities or individuals to the competent authorities (Reznik et al., 2021) relating to the existence of suspicious financial activity (Sultana, 2020) based on the applicable indicators and regulations (Williams, 2014). Meanwhile, the external function, where the FIU collaborates with various FIUs from other countries, provides effectiveness to the prevention of crypto laundering at the international level (Williams, 2014). FIU plays a role in conducting information exchange from one country to another country (FIU-to-FIU) through the application of an open database based on bilateral or

multilateral agreements from each country that exchanges FIU-to-FIU information (FATF, 2003).

RQ1: How is the RegTech-based anti-crypto laundering mechanism in Indonesia?

RQ2: What is the role of the FIU in Indonesia's anti-crypto laundering mechanism?

Research Method

This article presents a system-based (RegTech) crypto laundering prevention mechanism in Indonesia based on the rules and regulations that have been established and published by the Commodity Futures Trading Regulatory Agency. The study was conducted through a qualitative approach (Saunders et al., 2012), which was sourced from secondary data. A deeper analysis of secondary data aims to provide additional knowledge, interpretations, and conclusions that are different from previous findings (Bulmer et al., 2009). The research procedure carried out in this study is shown in Figure 4.

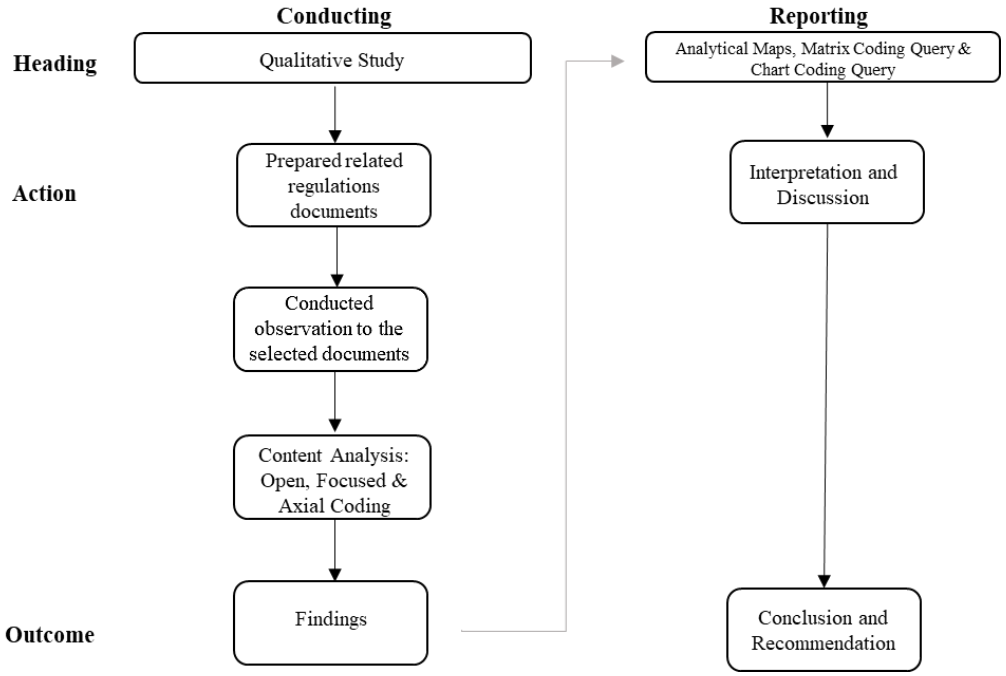


Figure 4. Research Procedure
Source: Authors (2023)

The secondary data used in this study are presented in Table 4.

Table 4 Secondary Data Sources

No	Regulation	Explanation
1.	Head of CFTR Regulation Number 8 of 2021 *(Peraturan Kepala Bappebti Nomor 8 Tahun 2021)*	Guidelines for the Implementation of Crypto Assets on the Futures Exchanges
2.	CFTR Regulation Number 5 of 2019 *(Peraturan Bappebti Nomor 5 Tahun 2019)*	Technical Provisions for the Implementation of the Crypto Asset on the Futures Exchange
3.	Head of CFTR Regulations and Attachment Numer 11 of 2017 *(Peraturan dan Lampiran Peraturan Kepala Bappebti Nomor 11 Tahun 2017)*	Guidelines for the Implementation of Anti-Money Laundering and Countering the Financing of Terrorism in Futures Brokers
4.	Head of CFTR Numer 8 of 2017 *(Peraturan Kepala Bappebti Nomor 8 Tahun 2017)*	Implementation of Anti-Money Laundering and Countering the Financing of Terrorism in Futures Brokers

Source: Authors (2023)

Furthermore, the data was analyzed using a content analysis approach (Holsti, 1969) or qualitative content analysis through a coding process with the aim of reducing data based on predetermined categories (Molinari & de Villiers, 2021). The secondary data coding process was carried out using NVivo with three stages of coding, namely: 1) Open coding (Corbin & Strauss, 2008), initial data analysis with focus categorization and simplified data structure; 2) Focused coding (Charmaz, 2006), reviewing and re-analyzing data—in the open coding stage—to group it into significant categories; and 3) Axial coding (Corbin & Strauss, 2008), finding the relationship between significant data categories as a process of theoretical development.

The data analysis technique with a qualitative content analysis approach employed by authors refers to Shi et al. (2022) and Silva (2022). The authors combined the techniques of two studies, where Shi et al. (2022) conducted the qualitative content analysis with the support of NVivo, while Silva (2022) applied open coding and axial coding in conducting data reduction in her qualitative content analysis approach. The authors added focused coding (Charmaz, 2006) as a codification technique to provide a piece of comprehensive systematic information on data analysis results (Saunders et al., 2012).

Result and Discussion

All of the crypto asset trading activities in Indonesia are supervised by the Commodity Futures Trading Regulatory Agency (CFTR), so the prevention of crypto laundering is currently regulated, established, and supervised by CFTR. Referring to the data analysis results presented in Appendix 1, CFTR regulates and establishes that crypto laundering prevention is carried out through Know Your Customer (KYC) and transaction monitoring based on a risk-based approach and RegTech-based. Especially for transaction monitoring activity, crypto asset trading platform operators (crypto FinTech) should report to the Indonesian Transaction Report and Analysis Center (INTRAC), which acts as the FIU in Indonesia. The data analysis results in this study are reported through analytical maps to

show the relationship of each finding, and through matrix and chart coding queries to show the amount of total coding processed on data sources. The visualization of the data is presented in the Appendix at the end of this article.

RegTech-based Crypto Laundering Prevention

Currently, cryptocurrency's growth is global; countries such as the United States, United Kingdom, Germany, Australia, and Japan are becoming major centers for virtual asset exchanges (Kirkpatrick et al., 2021). In Indonesia, the virtual asset (crypto) customer growth over the past three years has continued to increase. As of October 2023, the number of crypto asset customers was 18.06 million with a transaction value of IDR 104.9 trillion (Tempo, 2023). As such, regulation of virtual assets becomes an important thing for regulators because it is classified as an instrument of the riskiest investment (Kirkpatrick et al., 2021), neither the risk of loss that threatens investors nor the risk of money laundering that threatens the law.

This study revealed the process of preventing crypto laundering based on the applicable regulations in Indonesia. Based on the content analysis with the support of NVivo 12, it was found that the regulation in the use of virtual assets (crypto) and the process of preventing crypto laundering are presented in Table 5. The coding presented in Table 5 refers to the results of data analysis contained in Appendices 2 and 3.

Table 5 RegTech-based Anti-Crypto Laundering Mechanism Matrix Category

Main Categories	Sub-Categories	Code
Risk-Based Approach	a. Identify the risk understanding and assessment b. Risk tolerance c. Risk reduction and control d. Risk residual evaluation e. Implementation of a risk-based approach f. Risk-based approach review and evaluation	a. Risk mapping b. Establishment of risk limits c. Internal control and risk mitigation d. Ensuring the residual risk level is not higher than the risk tolerance e. Risk-based approach cycle documentation f. The effectiveness assessment of crypto laundering prevention program implementation
Know Your Customer	Customer Due Diligence or Enhanced Due Diligence	• Based on a risk-based approach • RegTech-based with face recognition features and liveliness characteristics • Data identification and verification integrated with the Ministry of Home Affairs's biometric data.
Transaction Monitoring	-	• Implement the Know Your Transaction (KYT) • Verification of withdrawals or transfers • Using blockchain analytic tools

Source: NVivo 12, Processed (2023)

In Indonesia, the use of virtual assets (crypto) is limited to trading on futures exchanges and not as a medium exchange. This restriction of use aligns with the regulations in Germany. In Germany, the use of crypto assets is only permitted for trading and is invalid as a medium of exchange (Kirkpatrick et al., 2021). The regulation of crypto asset trading in Germany is the duty and responsibility of the Federal Financial Supervisory Authority (BaFin/*Bundesanstalt für Finanzdienstleistungsaufsicht)* as the centralized regulator. Likewise, in the UK and Japan, the regulation of virtual asset trading is the duty and responsibility of the Financial Conduct Authority (FCA) and Japan's Financial Service Authority (JFSA).

Meanwhile, in Indonesia—at the time of reporting this study—it was found that the regulation of virtual asset trading is still the duty and responsibility of CFTR (Commodity Futures Exchanges Regulatory Agency). Reflecting on Germany, the UK, and Japan, the regulation of virtual asset trading in Indonesia should be the duty and responsibility of the Financial Services Authority *(Otoritas Jasa Keuangan)*. FSA has a function to organize an integrated regulatory and supervisory system for all financial activities in the financial services sector so that all activities related to virtual asset (crypto) trading should be under FSA's regulation and supervision. As for the prevention of money laundering involving virtual assets, the findings revealed that the prevention process in Indonesia is carried out by implementing KYC (Know Your Customer) and transaction monitoring.

In carrying out KYC activities, the study uncovered that organizations should use RegTech-based technology that applies face recognition with liveliness characteristics and is integrated with biometric data or population administration data owned by the Ministry of Home of Affairs. This finding is consistent with previous research that the RegTech utilization in the KYC process is crucial to preventing financial crime (Kurum, 2020). However, the application of face recognition with biometric data raises new issues related to data privacy. A study conducted by Liyanaarachchi et al. (2023) revealed that biometric data collection can harm individuals because it reduces individual control over their personal data and gives full authority to the organization in using their data. Although the biometric data collected by organizations is integrated with the Ministry of Home Affairs' biometric data, this does not make it legal and free from privacy imbalance issues (Liyanaarachchi et al., 2023). Instead, it implies new privacy concerns. Granting access to data owned by the Ministry of Home Affairs to organizations has a high potential to bring the Ministry of Home Affairs into violation of ethical guidelines for the use of technology that prioritizes privacy (Ryan & Stahl, 2021). Therefore, regulators need to review regulations and guidelines for data collection in the KYC process that can assure individuals that data collection is carried out based on ethical, security, and data privacy guidelines. Also, it is to avoid excessive, non-purposeful, inaccurate, and irrelevant data collection (Sarabdeen, 2023). Data privacy regulation should be an integral part of the technology adoption process by linking legal and regulatory considerations as core components of data privacy (Akanfe et al., 2024).

Meanwhile, in carrying out transaction monitoring, it was found that organizations are required to use blockchain analytic tools because the transactions involving crypto assets are decentralized with the application of blockchain technology. In line with Bhatt et al. (2020), the application of blockchain technology integrated with other technologies, such

as artificial intelligence (AI), has provided additional benefits and investment in blockchain technology. The authors did not find more details of the mechanism applied in blockchain analytic tools based on regulations in Indonesia. However, the authors expect that the mechanism used must be able to analyze the consensus algorithms mechanism, which is the core technology of blockchain (Bamakan et al., 2021). Some of the most important consensus algorithms in blockchain technology are proof of work, proof of stake, and proof of elapsed time (Bamakan et al., 2020). Those three consensus algorithms are interrelated in forming a chain of transaction blocks on the blockchain because they play a role in validating transactions, reading the amount of wealth mined, and securing transactions. Thus, the authors expect that blockchain analytic tools regulated in Indonesia use those three consensus algorithms as the basis for analyzing and defining the anomalous crypto asset transaction that occurred on the blockchain, along with the blockchain address associated with the transaction.

Nevertheless, every new technology has and faces its challenges. Blockchain is a relatively new technology; according to Bamakan et al. (2021), blockchain faces the challenge of energy consumption, where the energy used by blockchain is quite high, so blockchain plays a role in depleting energy resources. Hence, to prevent environmental degradation that can be a disruption of sustainable development, regulators need to collaborate with experts to review the real impact of blockchain technology on energy resources and then start considering regulating the use of renewable energy that is environmentally friendly.

KYC and transaction monitoring processes that are regulated through Indonesian regulations must be implemented by referring to the risk-based approach policy; thus, crypto FinTech must conduct a risk assessment. This finding corroborates the findings in the process of preventing crypto laundering in other countries, such as the UK and Bermuda (Kirkpatrick et al., 2021). Generally, the applicable regulations in Indonesia, the UK, and Bermuda regulate the prevention of crypto laundering, which must be implemented through the risk assessment, KYC, and transaction monitoring process. However, when comparing specifically, there are differences in the regulations of those three countries.

In the UK, education and training of human resources (HR)— directly involved in the prevention of crypto laundering—is part of the regulation of crypto laundering prevention mechanisms (Kirkpatrick et al., 2021). Meanwhile, in Indonesia, it has not yet become part of the regulation. Currently, the regulation of crypto laundering prevention still regulates the system technically and has not regulated the human resources involved. The regulations only regulate the requirements for selecting HR through the KYE (Know Your Employee) process, which is carried out before HR engages with the organization. The absence of the role of regulations and regulators in HR management has implications for the low level of crypto FinTech awareness of the crypto laundering risk.

In comparison, in Bermuda, regulations require organizations to conduct periodic testing of their crypto laundering prevention procedures, whether those procedures are still relevant and adequate in dealing with any problems (Kirkpatrick et al., 2021). In Indonesia, this is not regulated. The absence of provisions regarding periodic review examination is a deficiency that has implications for weakening the enforcement of crypto laundering

preventing regulations. The application of the applicable regulations in the UK and Bermuda can provide insight to regulators and parties involved that the regulations applicable in Indonesia currently still need to be reviewed and re-optimized because safe regulations should be able to cover all elements related to the prevention of crypto laundering and can predict events that may occur in the future (McCarthy, 2022).

Financial Intelligence Unit's Role in Crypto Laundering Prevention

The role of the Financial Intelligence Unit (FIU) is to collect, analyze, and disseminate reports on entities or individuals (Reznik et al., 2021) related to suspicious financial activity (Sultana, 2020). In Indonesia, research findings reveal that this role is carried out by the Indonesia Transaction and Report and Analysis Center (INTRAC) as an independent institution to prevent and eradicate all forms of money laundering by collaborating with other parties (anti-money laundering regime) and forwarding the results of its analysis to law enforcement agencies. Based on a study conducted by McNaughton (2023), by comparing various FIU models of Western countries (Canada, Denmark, Netherlands, Luxemburg, United States) and Eastern countries (Estonia, Latvia, Lithuania, Poland, Ukraine), it was found that the FIU is a national institution that is not homogeneous. This is because, on a normative basis, the scope of FIU activity is determined by the respective domestic anti-money laundering framework. The results of this study indicate that the scope of the FIU's role between one country and another can be different. McNaughton (2023) also found that typically, countries establish FIUs with one of two main models, namely the administrative or the law enforcement FIU. In the administrative model, the FIU's functions typically provide the information needed (tactics intelligence) to investigators or law enforcement and act as a supervisor to ensure AML compliance from reporting parties or financial institutions. In this model, FIU does not have any authority and power to conduct investigations. Whereas in the law enforcement model, the FIU has the authority to conduct investigations, seize suspicious transactions, and conduct law enforcement. This model is typically granted to a special police unit. However, several countries establish a third type of FIU: judicial FIU, which is a specialized unit within the Attorney General's Office and combines the features of the administrative and law enforcement type FIU. Others countries establish a hybrid model by combining features in the administrative, law enforcement, and judicial FIU.

In Indonesia, the findings in this study do not provide any indication that Indonesia applies any of the four FIU models. The scope of INTRAC's role and authority does not include the authority to oversee compliance functions and conduct law enforcement, and INTRAC is not under the Attorney General's Office or a specialized unit within the police. INTRAC is under and directly responsible to the president and submits periodic reports on the implementation of its authority to the president and the House of Representatives. However, FIUs are not homogeneous, so there are no standard provisions in determining the FIU model that must be applied to each country. The FIU model adopted by Indonesia refers to the normative basis of the AML framework in Indonesia.

In the anti-crypto laundering framework, the research findings uncover that INTRAC has the role and right to receive reports from crypto FinTech on suspicious transactions based on the results obtained through the application of blockchain analytic tools (RegTech).

The information in the report is the result of integrating blockchain—as the underlying technology of crypto asset exchange—with artificial intelligence (AI) through the application of blockchain analytic tools. This finding is supported by the simulation results of the Integrated Blockchain and Artificial Intelligence Framework (IBAI Framework). The framework was proposed by Alenizi et al. (2024) and simulated the financial transactions. Based on the simulation, the IBAI Framework exhibits significant numerical results to increase the detection ratio of suspicious behaviors with an accurate rate of 98%. The optimization of blockchain analytic tolls application can basically have a positive impact on the credibility of reports received by INTRAC so that, ideally, it can facilitate INTRAC in carrying out its role to conduct further analysis of suspicious transactions. Based on the research findings, INTRAC conducts further analysis with a follow-the-money approach and forwards the results of the analysis to law enforcement agencies. However, when referring to the results of studies in other developing countries—such as Tanzania—electronic money laundering/crypto laundering becomes a challenge for FIUs in developing countries when FIUs do not have adequate tools and technology to conduct further analysis of suspicious transactions in blockchain (Mniwasa, 2019). It is possible that Indonesia, as a developing country, faces similar problems, so that can have implications for the existence of INTRAC's role in preventing and eradicating all forms of money laundering. Therefore, regulators/AML regimes need to ensure that INTRAC has adequate tools and technology to analyze various transactions with their underlying technologies. Likewise, the human resources assigned need to be filled by people with the relevant qualifications and knowledge. Tools, technology, and human resources representing INTRAC are closely related to the existence of INTRAC in carrying out its authority, whether it weakens or strengthens the role of INTRAC as the FIU in Indonesia.

Conclusion

This study reveals the mechanism established by CFTR in preventing crypto laundering. Generally, crypto laundering prevention consists of Know Your Customer (KYC) and transaction monitoring activities and is implemented based on a risk-based approach. Normatively, this prevention mechanism is implemented based on RegTech through face recognition for KYC and the application of blockchain analytic tools for transaction monitoring. The utilization of RegTech in Indonesia is carried out continuously with the role of INTRAC as the Financial Intelligence Unit (FIU). INTRAC is independent and directly responsible to the president. This study demonstrates that INTRAC has the right to receive suspicious transaction reports from financial institutions and has the authority to conduct further analysis of these transactions. INTRAC's success in analyzing suspicious transactions involving crypto assets depends on the capacity of its tool, technology, and human resources competencies. These three factors are important for INTRAC in maintaining the existence of its role as FIU and part of the anti-money laundering regimes in Indonesia. In preventing crypto laundering, Indonesia needs an FIU that plays a responsive and adaptive role in various developments in financial technology.

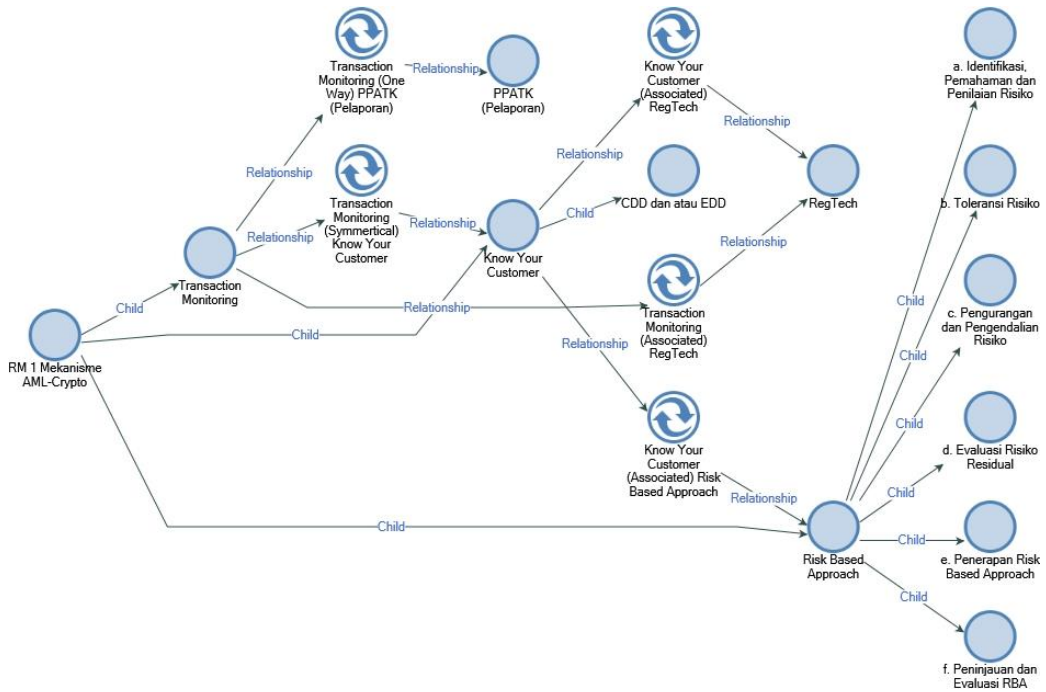
The authors highlight the crypto laundering prevention mechanism and the role of the FIU that have not been comprehensively established to provide theoretical insights and

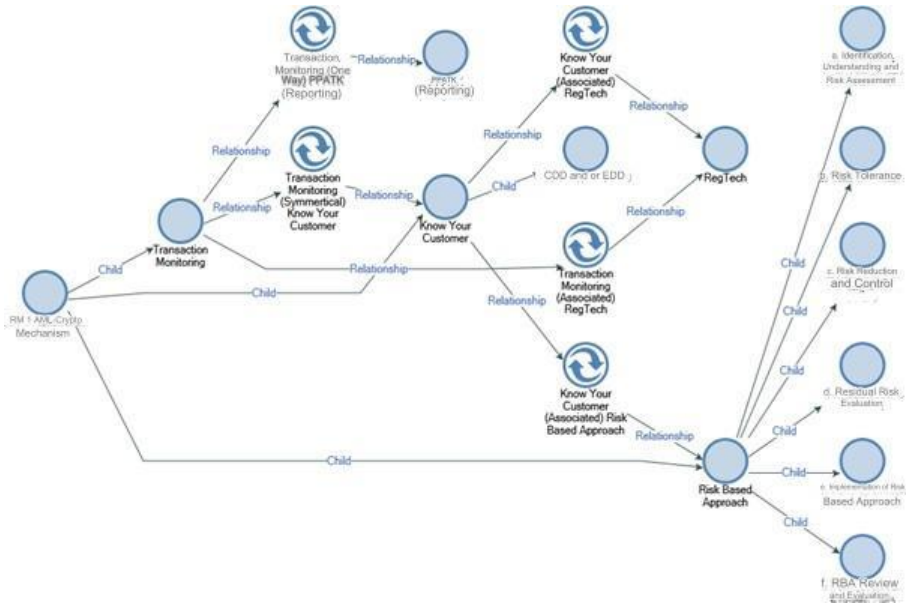
practical implications, encouraging the Commodity Futures Trading Regulatory Agency and the Financial Service Authority as stakeholders to re-examine and develop the crypto laundering prevention mechanism based on its underlying technologies, along with the parties of the anti-money laundering regime, and consider collaborating with experts from various fields.

This study has been conducted and monitored prudentially. However, the authors acknowledge that there are things beyond their control and can be an opportunity for future research. This research only relied on regulatory documents (secondary data), which still need to be optimized because they have not explained the whole mechanism of RegTech and FIU. Thus, the role of RegTech and FIU was only studied normatively. Future studies are expected to elaborate how the role of RegTech and FIU in preventing crypto laundering empirically and compare the empirical findings with the normative findings in this study.

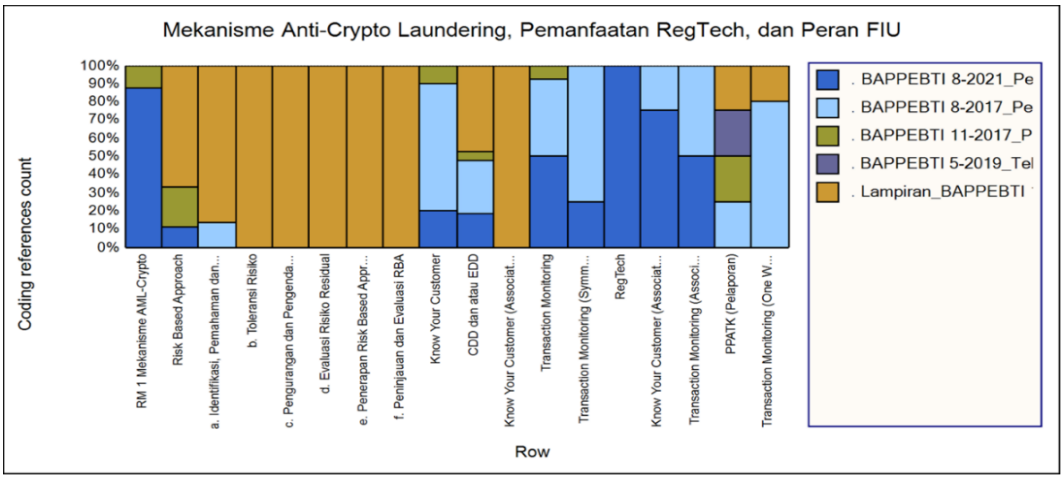
Appendix

Appendix 1 Analytical Maps – Crypto Laundering Prevention Mechanisms

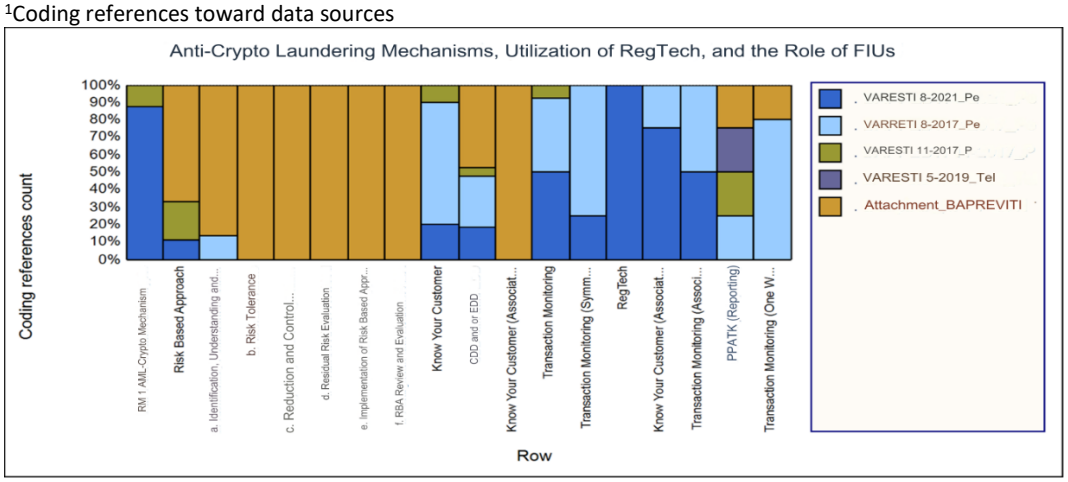




Appendix 2 Chart Coding Query[1] - Crypto Laundering Prevention Mechanisms



[1]Coding references toward data sources



Appendix 3 Matrix Coding Query[2] - Crypto Laundering Prevention Mechanisms

	A : BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	B : BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka	C : BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	D : BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto	E : Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka
1 : RM 1 Mekanisme AML-Crypto	7	0	1	0	0
2 : Risk Based Approach	1	0	2	0	6
3 : a. Identifikasi, Pemahaman dan Penilaian Risiko	0	2	0	0	13
4 : b. Toleransi Risiko	0	0	0	0	3
5 : c. Pengurangan dan Pengendalian Risiko	0	0	0	0	5
6 : d. Evaluasi Risiko Residual	0	0	0	0	4
7 : e. Penerapan Risk Based Approach	0	0	0	0	5
8 : f. Peninjauan dan Evaluasi RBA	0	0	0	0	4
9 : Know Your Customer	2	7	1	0	0
10 : CDD dan atau EDD	8	13	2	0	21
11 : Know Your Customer (Associated) Risk Based Approach	0	0	0	0	2
12 : Transaction Monitoring	13	11	2	0	0
13 : Transaction Monitoring (Symmertical) Know Your Customer	1	3	0	0	0
14 : RegTech	3	0	0	0	0
15 : Know Your Customer (Associated) RegTech	3	1	0	0	0
16 : Transaction Monitoring (Associated) RegTech	2	2	0	0	0
17 : PPATK (Pelaporan)	0	1	1	1	1
18 : Transaction Monitoring (One Way) PPATK (Pelaporan)	0	4	0	0	1

	A: BAPPEBTI 8-2021_Guidelines for Organizing Crypto Asset Trading on Futures Exchanges	B: BAPPEBTI 8-2017_Implementation of APU PPT Program in Futures Brokers	C : BAPPEBTI 11-2017_APU PPT Program at Futures Brokers	D: BAPPEBTI 5-2019_Technical Implementation of Physical Market for Crypto Assets	E: Attachment_BAPREVITI 11- 2017_APU PPT Program at Futures Brokers
1: RM 1 AML-Crypto Mechanism	7	0	1	0	0
2 : Risk Based Approach	1	0	2	0	6
3: a. Identification, Understanding and Risk Assessment	0	2	0	0	13
4: b. Risk Tolerance	0	0	0	0	3
5: c. Risk Reduction and Control	0	0	0	0	5
6: d. Residual Risk Evaluation	0	0	0	0	4
7: e. Implementation of Risk Based Approach	0	0	0	0	5
8: f. RBA Review and Evaluation	0	0	0	0	4
9 : Know Your Customer	2	7	1	0	0
10: CDD and or EDD	8	13	2	0	21
11 : Know Your Customer (Associated) Risk Based Approach	0	0	0	0	2
12 : Transaction Monitoring	13	11	2	0	0
13 : Transaction Monitoring (Symmertical) Know Your Customer	1	3	0	0	0
14 : RegTech	3	0	0	0	0
15 : Know Your Customer (Associated) RegTech	3	1	0	0	0
16 : Transaction Monitoring (Associated) RegTech	2	2	0	0	0
17: PPAT K (Reporting)	0	1	1	1	1
18 : Transaction Monitoring (One Way) PPAT K (Reporting)	0	4	0	0	1

[2] Total coding of each data sources

References

Adachi, D., & Aoyagi, J. (2020). Blockchain and Economic Transactions. *Cryptocurrency and Blockchain Technology*. https://doi.org/10.1515/9783110660807-002

Akanfe, O., Lawong, D., & Rao, H. R. (2024). Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities. *International Journal of Information Management*, *76*(August 2023), 102753. https://doi.org/10.1016/j.ijinfomgt.2024.102753

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*(November 2021), 1–30. https://doi.org/10.1016/j.techfore.2022.121632

Al-Tawil, T. N. (2022). Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-07-2022-0109

Albrecht, Duffin, K. M. K., Hawkins, S., & Morales Rocha, V. 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

Albrecht, W., Albrecht, C., Albrecht, C., & Zimbelman, M. (2012). *Fraud Examination* (4th ed.). Cengage Learning South-Western.

Alenizi, A., Mishra, S., & Baihan, A. (2024). Enhancing secure financial transactions through the synergy of blockchain and artificial intelligence. *Ain Shams Engineering Journal*, *October 2023*, 102733. https://doi.org/10.1016/j.asej.2024.102733

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

Bamakan, S. M. H., Babaei Bondarti, A., Babaei Bondarti, P., & Qu, Q. (2021). Blockchain technology forecasting by patent analytics and text mining. *Blockchain: Research and Applications*, *2*(2), 100019. https://doi.org/10.1016/j.bcra.2021.100019

Bamakan, S. M. H., Motavali, A., & Bondarti, A. B. (2020). A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria. *Expert Systems with Applications*, *154*.

Basel Institute of Governance. (2021). Basel AML Index 2021 : 10th Public Edition Ranking money laundering and terrorist financing risks around the world. *Annual Report*.

Bhatt, P. C., Kumar, V., Lu, T.-C., Cho, R. L.-T., & Lai, K. K. (2020). Rise and Rise of Blockchain: A Patent Statistics Approach to Identify the Underlying Technologies. *Asian Conference on Intelligent Information and Database Systems*, 456–466.

Bulmer, M., Sturgis, P. J., & Allum, N. (2009). *Secondary Analysis of Survey Data*. SAGE.

Bylund, A. (2023). *What Is Blockchain?* The Motley Fool. https://www.fool.com/terms/b/blockchain/

Chainalysis. (2022). *The 2022 Crypto Crime Report* (Issue February). https://go.chainalysis.com/2022-crypto-crime-report.html

Charmaz, K. (2006). Constructing Grounded Theory. In *British Library*. SAGE.

Corbin, J., & Strauss, A. (2008). *Basics of Qualitative Research* (3rd ed.). SAGE.

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

FATF. (2003). *The Forty Recommendations*.

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

Finder. (2022). *Finder Cryptocurrency Adoption Index*. https://www.finder.com/id/finder-cryptocurrency-adoption-index

Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime*, *17*(4), 441–458. https://doi.org/10.1108/13590791011082797

Holsti, O. (1969). *Content Analysis for the Social Sciences*. Addison-Wesley.

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. 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

Kementerian Keuangan RI. (2022). *Menuju Era Uang Rupiah Digital*. https://djpb.kemenkeu.go.id/portal/id/berita/lainnya/opini/3950-menuju-era-uang-rupiah-digital.html

Kirkpatrick, K., Stephens, A., Gerber, J., Nettesheim, M., & Bellm, S. (2021). Understanding regulatory trends: digital assets & anti-money laundering. *Journal of Investment Compliance*, *22*(4), 345–353. https://doi.org/10.1108/joic-07-2021-0033

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

Litchfield, H. (2015). A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology. *Australian Computer Society*.

Liyanaarachchi, G., Viglia, G., & Kurtaliqi, F. (2023). Privacy in Hospitality: Managing Biometric and Biographic Data with Immersive Technology. *International Journal of Contemporary Hospitality Management*. https://doi.org/https://doi.org/10.1108/IJCHM-06-2023-0861

Lukito, A. S. (2016). Financial intelligent investigations in combating money laundering crime: An Indonesian legal perspective. *Journal of Money Laundering Control*, *19*(1), 92–102. https://doi.org/10.1108/JMLC-09-2014-0029

Mardiansyah. (2021). *Penilaian Risiko Indonesia Pencucian Uang*. Pusat Pelaporan dan Analisis Transaksi Keuangan.

McCarthy, J. (2022). The regulation of RegTech and SupTech in finance: ensuring consistency in principle and in practice. *Journal of Financial Regulation and Compliance*, *31*(2), 186–199. https://doi.org/10.1108/JFRC-01-2022-0004

McNaughton, K. J. (2023). The variability and clustering of Financial Intelligence Units (FIUs) – A comparative analysis of national models of FIUs in selected western and eastern (post-Soviet) countries. *Journal of Economic Criminology*, *2*(October), 100036. https://doi.org/10.1016/j.jeconc.2023.100036

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

Mniwasa, E. E. (2019). The financial intelligence unit and money laundering control in Tanzania: The law, potential and challenges. *Journal of Money Laundering Control*, *22*(3), 543–562. https://doi.org/10.1108/JMLC-07-2018-0043

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

Moore, M. (2018). *Everything You Need to Know About Blockchain*. Albawaba. https://www.albawaba.net/business/everything-you-need-know-about-blockchain-1158228

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

Otoritas Jasa Keuangan. (2022). *Peran Regtech dalam Mendukung Kinerja Lembaga Jasa Keuangan*. https://www.ojk.go.id/ojk-institute/id/capacitybuilding/upcoming/229/peran-regtech-dalam-mendukung-kinerja-lembaga-jasa-keuangan

Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 5: Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka, (2019).

Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka, (2021).

Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 11 Lampiran: Pedoman Penerapam Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme pada Pialang Berjangka, (2017).

Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme pada Pialang Berjangka, (2017).

Peters, G. W., Panayi, E., & Chapelle, A. (2015). Trends in Cryptocurrencies and Blockchain Technologies: a Monetary Theory and Regulation Perspective. *The Journal of Financial Perspectives: FinTech*, *3*(3).

Pickett, K. H. S., & Pickett, J. (2002). *Financial Crime Investigation and Control*. Wiley.

Pontes, R., Lewis, N., McFarlane, P., & Craig, P. (2022). Anti-money laundering in the United Kingdom: new directions for a more effective regime. *Journal of Money Laundering Control*, *25*(2), 401–413. https://doi.org/10.1108/JMLC-04-2021-0041

Reznik, O., Utkina, M., & Bondarenko, O. (2021). Financial intelligence (monitoring) as an effective way in the field of combating money laundering. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-09-2021-0102

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

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*. Pearson Education Ltd., Harlow.

Seebacher, S., & Schüritz, R. (2017). Blockchain technology as an enabler of service systems: a structured literature review. *8th International Conference on Exploring Services Science*, 12–23.

Shi, X., Yao, X., Liang, J., Gan, S., & Li, Z. (2022). China's cultivation of master nursing specialist: A qualitative content analysis of the stakeholders. *Nurse Education in Practice*, *63*(May), 1–7. https://doi.org/10.1016/j.nepr.2022.103359

Silva, D. (2022). Pre-service teachers' understanding of culture in multicultural education: A qualitative content analysis. *Teaching and Teacher Education*, *110*, 1–11. https://doi.org/10.1016/j.tate.2021.103580

Singh, C., & Lin, W. (2021). Can artificial intelligence, RegTech and CharityTech provide effective solutions for anti-money laundering and counter-terror financing initiatives in

charitable fundraising? *Journal of Money Laundering Control*, *24*(3), 464–482. https://doi.org/10.1108/JMLC-09-2020-0100

Singh, C., Zhao, L., Lin, W., & Ye, Z. (2022). Can machine learning, as a RegTech compliance tool, lighten the regulatory burden for charitable organisations in the United Kingdom? *Journal of Financial Crime*, *29*(1), 45–61. https://doi.org/10.1108/JFC-06-2021-0131

Sultana, S. (2020). Role of financial intelligence unit (FIU) in anti-money laundering quest: Comparison between FIUs of Bangladesh and India. *Journal of Money Laundering Control*, *23*(4), 931–947. https://doi.org/10.1108/JMLC-01-2020-0003

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

Tempo. (2023). *Tren Investor Aset Kripto Meningkat Sepanjang 2023, tapi Nilai Transaksi Menurun*. https://bisnis.tempo.co/read/1805369/tren-investor-aset-kripto-meningkat-sepanjang-2023-tapi-nilai-transaksi-menurun

Utami, A. M., & Septivani, M. D. (2022a). 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. (2022b). 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

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

Williams, C. (2014). Artificial harmony: Why cooperative efforts to create a global financial intelligence unit have faltered. *Journal of Money Laundering Control*, *17*(4), 428–439. https://doi.org/10.1108/JMLC-08-2013-0030

Wronka, C. (2022a). 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. (2022b). "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. (2022c). 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

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

Zaman, A., Tlemsani, I., Matthews, R., & Hashim, M. A. M. (2023). Assessing the potential of blockchain technology for Islamic crypto assets. *Competitiveness Review*. https://doi.org/10.1108/CR-05-2023-0100

About the Authors

Kharisma Fatmalina Fajri (K.F.F.) is an Alumni of the Accounting Master's Program, Faculty of Business and Economics, Universitas Islam Indonesia, Sleman, Special Region of Yogyakarta, Indonesia. She can be reached via email at kharismaffajri@gmail.com.

Dekar Urumsah (D.U.) is an Associate Professor in the Accounting Department, Faculty of Business and Economics, Universitas Islam Indonesia, Sleman, Special Region of Yogyakarta, Indonesia. He can be reached via email at 933120101@uii.ac.id.

Author Contributions

Conceptualisation, K.F.F. and D.U.; Methodology, K.F.F.; Investigation, K.F.F. and D.U.; Analysis, K.F.F.; Original draft preparation, K.F.F. and D.U.; Review and editing, K.F.F and D.U.; Visualization, K.F.F.; Supervision, D.U.

Conflicts of Interest

The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.