Financial Intelligence Units and Regulatory Technology to Combat Crypto Laundering

Mehedi Hassan Murad[1], Imran Uddin[2], Sadia Maliha Trisha[3], Shuvo Kumar Mallik[4], Md. Kabirul Islam[5], Noushin Akhter Nova[6]

[1]Department of Finance and Banking, National University, Dhaka, Bangladesh

[2]A2Z Finance Australia (Easy Mortgage Solutions Australia), Australia.

[3]Dublin Business School, Dublin, Ireland.

[4]Department of Economics, Southeast University, Dhaka, Bangladesh

[5]Lecturer, Department of Finance and Banking, Uttara Town College, Dhaka, Bangladesh

[6]Country Advisory, International Finance Corporation (IFC).

DOI: https://dx.doi.org/10.47772/IJRISS.2025.915EC0010

Received: 30 January 2025; Accepted: 08 February 2025; Published: 20 February 2025

ABSTRACT

Since digital payments increased in 2015, crypto laundering has become a significant threat. This study explores preventing crypto laundering through RegTech and FIU, using qualitative content analysis with NVivo 12. Legal documents from the Commodity Futures Trading Regulatory Agency (CFTR) served as secondary data sources. Crypto laundering mitigation includes KYC (Know Your Customer) and risk-based transaction monitoring. Customized RegTech solutions, like facial recognition technology, should complement blockchain analytics tools. The study found that government agencies issue suspicious transaction reports, while INTRAC, Indonesia's financial institution unit, handles transaction monitoring and analysis using a "follow the money" methodology. This research contributes to forensic accounting knowledge and suggests policy-level actions for regulators, collaborating with technology specialists to combat crypto laundering.

Keyword: Crypto Laundering; Blockchain; RegTech; Financial Intelligence Unit

INTRODUCTION

Money laundering (ML) is an intangible process that conceals the source of profits earned from illegal activities (Gottschalk, 2010). It strengthens the application of ML which refers to blocking the profit of the illegal commitment by the offender (Pontes et al., 2022). In arithmetic, the predicate crime (fraud, corruption, and theft) undergoes the process of concealment (Pickett & Pickett, 2002; Larkin, S. B. 2025) and conversion process (Albrecht et al., 2012); thus, ML has been an important activity in financial crime (Gottschalk, 2010). ML activities are designed to facilitate the use of 'illicit funds' legally by the criminal (Gottschalk, 2010); hence the proceeds of those activities are integrated with lawful economic processes as the objective of ML is to convert unlawful proceeds into lawful ones. Therefore, in relation to this typology and ecosystem, the nature of the anti-money laundering (AML) system itself should be responsive and preventive of various methods of ML that occur, given that human lifestyles and technological advances influence the very dynamics of activities such as ML (Wronka, 2022a).

Technological innovations, digitalization and the internet penetration have significantly influenced the operations of ML perpetrators steal digitalization technologies that provide new opportunities to commit ML with the most modern techniques (Mugarura & Ssali, 2020) (online transactions (cyber laundering) and use digital payments and virtual currencies. Money laundering using virtual currencies allows avoiding detection of law enforcement officials and complicating identification (Wronka, 2022a; Wronka, 2022b; Mardiansyah, 2021). Cyber laundering is supposed to make the detection quite hard as it operates in more than one currency

(multi-currency), where the perpetrators use crypto currencies that are easy to use, relatively anonymous, hard to trace, and are not bound by law and regulation (van Wegberg et al., 2018; Leuprecht et al., 2022). For the placement and layering stages, they use cryptocurrencies, but in the integration stage they use fiat currencies (Leuprecht et al., 2022). The trend of using cryptocurrencies for ML purposes is also increasing, as the number of such cases grew exponentially: 30% increase by year 2021 (Chainalysis, 2022), and rising according to newest data (Dyntu & Dykyi, 2019). Finder (2022) noted that as of October 2023, crypto users and owners made up 15% of the population in Canada, where the average was 14% of the population globally. Futures exchanges have determined that the underlying of cryptocurrency and crypto assets are commodities (Jakfar, 2022), yet they are not a legal tender because it is not being controlled by the local monetary authority (central bank) (Kementerian Keuangan RI, 2022). There has been an emerging threat known as virtual currency (cryptocurrency) to ML. It is used in trade activities with the account being used for others, ecommerce misappropriates a transaction from the proceeds of crime, unlicensed peer-toper lending on financial technology activities, and used in digital currency networks online black-market transactions from the proceeds of tax crime and online gambling with medium ML risk (Mardiansyah, 2021).

To address these challenges which hinder AML systems and amplify threats to regional and global economic stability, the Financial Action Task Force (FATF) provides recommendations to their member states to ensure that virtual asset providers are registered with local monetary authority as well as to follow the AML systems for risk mitigation and to stop money laundering through virtual assets (FATF, 2022). Virtual assets have been used in illicit activities in over 37 million transactions/year (Leuprecht et. al, 2022), hence producing a huge amount of data. Financial institution's compliance with AML systems and suspicious transaction reporting becomes more expensive and complex because of the sheer quantity and abundance of data (Teichmann et al., 2022). Thus, the acceptance of regulatory technology (RegTech) using digital automation with the latest version is a practical solution to avoid ML related to virtual assets (crypto laundering) (Teichmann et al., 2022). Some of the newest technologies in RegTech have been confirmed as controlling and analytical assistance (Zabelina et al., 2018), including machine learning (Singh et al., 2022; Ruiz & Angelis, 2021), artificial intelligence (Singh & Lin, 2021; Kurum, 2020), and cloud computing (Kurum, 2020). In preventing crypto laundering, RegTech alone does not suffice, it must also be aligned with an independent role of the FIU to receive and follow up on every suspicious transaction from financial institutions (Lukito, 2016; Naheem, 2018). It was directly supervised by the head of FIU to provide some synergy between FIU and financial institutions in addressing a number of obstacles faced in the ML effort (Lukito, 2016).

There are various studies focused on the topic of cryptocurrency and crypto asset (Leuprecht et al., 2022; Wronka, 2022c; Akartuna et al., 2022; Albrecht et al., 2019; Dyntu & Dykyi, 2019; van Wegberg et al., 2018), which are able to confirm that cryptocurrency and crypto asset are participating in the money laundering to some extent, in particular during the placement and layering stage of the process. RegTech studies (Utami & Septivani, 2022b; Utami & Septivani, 2022a; Meiryani et al., 2022; Kurum, 2020; Naheem, 2018; Anagnostopoulos, 2018) suggested the ability of RegTech and its underlying technologies in fighting financial crime made them impactful technologies for financial institutions, however some other studies still found insignificant results due to inhibiting factors. Then studied the financial intelligence and FIU role (Reznik et al. 2021; Sultana 2020; Lukito 2016), which emphasized the importance of financial intelligence and FIU role in combating financial crimes and the lack of FIU's role may accelerate the exchange of cash from financial crimes. Only Ruiz and Angelis (2021) conducted a study that particularizes the use of RegTech in preventing crypto laundering, by investigating machine learning in preventing crypto laundering and showing the results through machine learning----that it can help to narrow down the crypto laundering, but the implementation of decision making in the machine learning still needs further improvement. So that study of RegTech is used in the system of Anti-Crypto Laundering is considered in a narrower manner by incorporating the role of the FIU, which is conducting supervision in the Anti-Crypto Laundering (Sultana, 2020).

Therefore, this study attempts to unveil the mechanism of crypto laundering prevention, focusing on the RegTech utilization for this purpose and the role of FIU, which is still evolving and improving (Otoritas Jasa Keuangan, 2022). This study elaborates the laws and regulations published by the Commodity Futures Trading Regulatory Agency (CFTR). Then, theoretical elaboration on RegTech and FIU in crypto laundering prevention is established as part of the analysis process. In addition, the mechanism of the concept of RegTech based crypto

laundering prevention and role of FIU in the crypto laundering prevention mechanism will be completed by discussing the influence of RegTech's underlying technologies on data privacy and on environmental sustainability as well as discussion on enhancement of the existence effect of Transaction Report and Analysis Center/INTRAC itself as FIU.It is significant in the area of forensic accounting, especially on the subject of money laundering. The content of the study contemplates modern contemporaneous accounting questions, but they also show their connection with other branches of science. This study also presents the practical implications for the Commodity Futures Trading Regulatory Agency and Financial Service Authority as stakeholders. These study findings also elucidate how regulators engage with different experts from information technology and environmental domains to formulate regulations and policies to combat crypto laundering.

LITERATURE REVIEW

RegTech with Financial Intelligence Unit for Countering Crypto Laundering

A crypto asset, or cryptocurrency, is a type of virtual currency that Satoshi Nakamoto implemented in 2009, serving as a type of currency in cryptocurrencies (Albrecht et al., 2019). This virtual currency is not issued and not limited by a country (stateless) and intangible by using blockchain as a virtual ledger technology that can maintain the stability of the currency value (Adachi & Aoyagi, 2020) unlike fiat currencies that are legally issued by a country. As every cryptocurrency transaction consists of a chain of codes in a virtual ledger and every transaction gets verified through the blockchain, the stability of the currency value can be ensured (Litchfield, 2015).

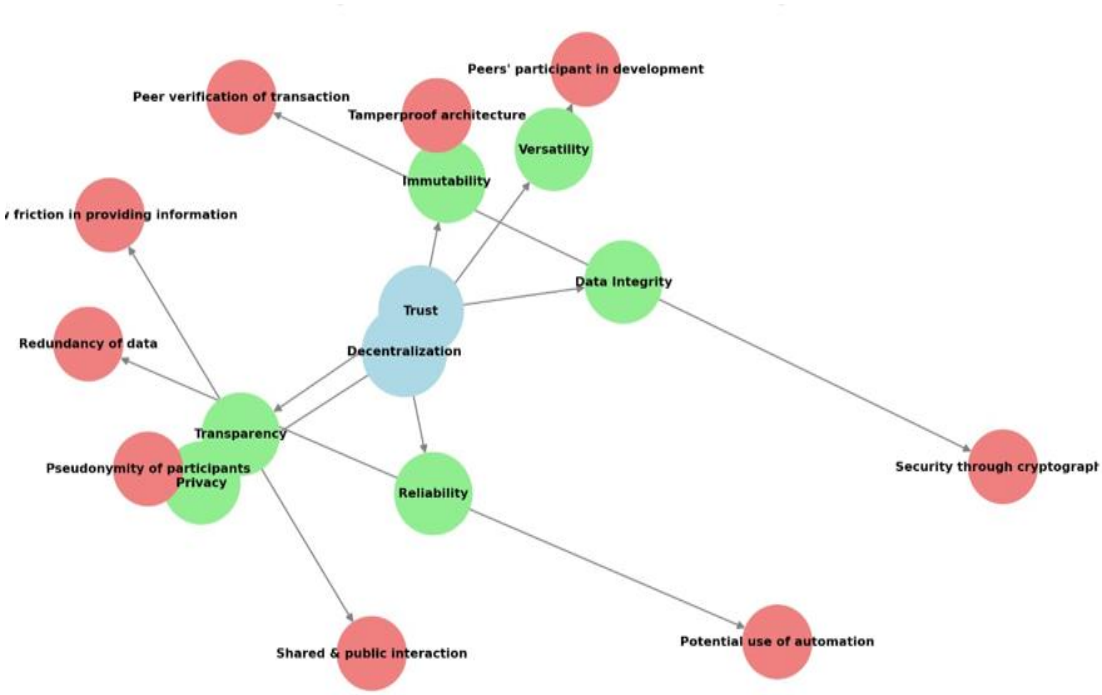


Figure 1 Characteristics of Blockchain Technology

Because blockchain is open public, the transactions which are encrypted then verified are every cryptocurrency candidate and not transactions of every individual or organization with a goal to compile a 'blockchain' and not compile transactions belonging to each individual or organization (Albrecht et al., 2019). Each blockchain block stores a cryptographic hash (a set of cryptographic codes) of the immediately previous block, with the hash being produced by taking the previous block's data and converting it into a compact string (Zaman et al., 2023). Hence, the string is unfeasible, consequently the block connection makes the chains digital currency sure and decentralized (Zaman et al., 2023), There is no specify server which hold exchange. As a result, each block must satisfy the chain conditions whereby no transaction could supersede the preceding transaction (Moore, 2018). In addition to the decentralized characteristics of blockchain technology, it is also trusting characteristics (Seebacher & Schüritz, 2017). This is specified and further divided into attributes as seen in **Figure 1** (Seebacher

& Schüritz, 2017). The latter is illustrated in **Figure 2,** which shows how transactions that happen in blockchain technology get recorded to construct a 'blockchain' (Bylund, 2023).

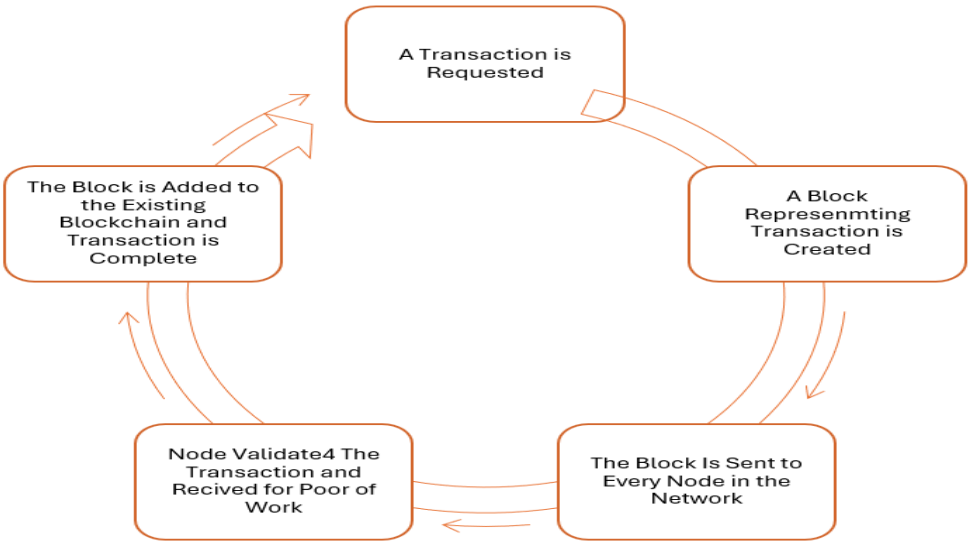


Figure 2 Transaction Recording Process in Blockchain

Table 1 presents fundamental differences between fiat currencies and cryptocurrencies in the context of payment transactions (Wronka, 2022c). Cryptocurrency transactions do not inherently require banks or other intermediary institutions and financial transaction owners remain relatively anonymous (Peters et al., 2015; van Wegberg et al., 2018; Albrecht et al., 2019; Leuprecht et al., 2022; Al-Tawil, 2022). Consequently, financial criminals began taking advantage of cryptocurrencies throughout the ML process (Albrecht et al., 2019). Due to their stateless property, the decentralized nature nature of cryptocurrencies and lack of a governing body with authority, perpetrators can easily transfer money from one country to another country in the network of cryptocurrencies with only an internet connection (Albrecht et al., 2019). Cryptocurrencies endanger the security of the world financial system with such ease (Al-Tawil, 2022). According to recent data 30% of ML activities in darknet markets were carried out using cryptocurrencies from 2020 to 2021, which does not include ML activities via cryptocurrencies that are also used in combination with fiat currencies (Chainalysis, 2022). The integration of crypto-fiat currencies through conversion of fiat currencies to cryptocurrencies and vice versa is conducted by perpetrators to render 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

Similar to the traditional ML method, the ML technique with citizen science includes three fundamental stages which are placement, layering, and integration. First of all, placement is a critical stage and the starting point of following the money (Albrecht et al., 2019). At this point the offenders employ cryptocurrencies that are anonymous and hard to trace (Leuprecht et al., 2022). The mindset of perpetrators is converting fiat money gained from illegal sources into cryptocurrency (Wronka, 2022c).

Second, layering, perpetrators will use cryptocurrencies in various jurisdictions through trading and investing or exchanging coins with other types of cryptocurrencies due to the virtual and stateless nature of cryptocurrencies (Leuprecht et al., 2022). This approach is known as chaining of transactions (Wronka, 2022c). Another frequently used method is the mixer method, which works as it combines multiple transactions and distributes them to multiple wallets which allows for greater difficulty in tracing the transactions to the actual source of funds (Wronka, 2022c). Third, perpetrators need to integrate gained cryptocurrencies with fiat currencies (Leuprecht et al., 2022; Albrecht et al., 2019) to make it possible to use ML proceeds in the legal monetary circulation (Wronka, 2022c). **Figure 3** Crypto Laundering Process

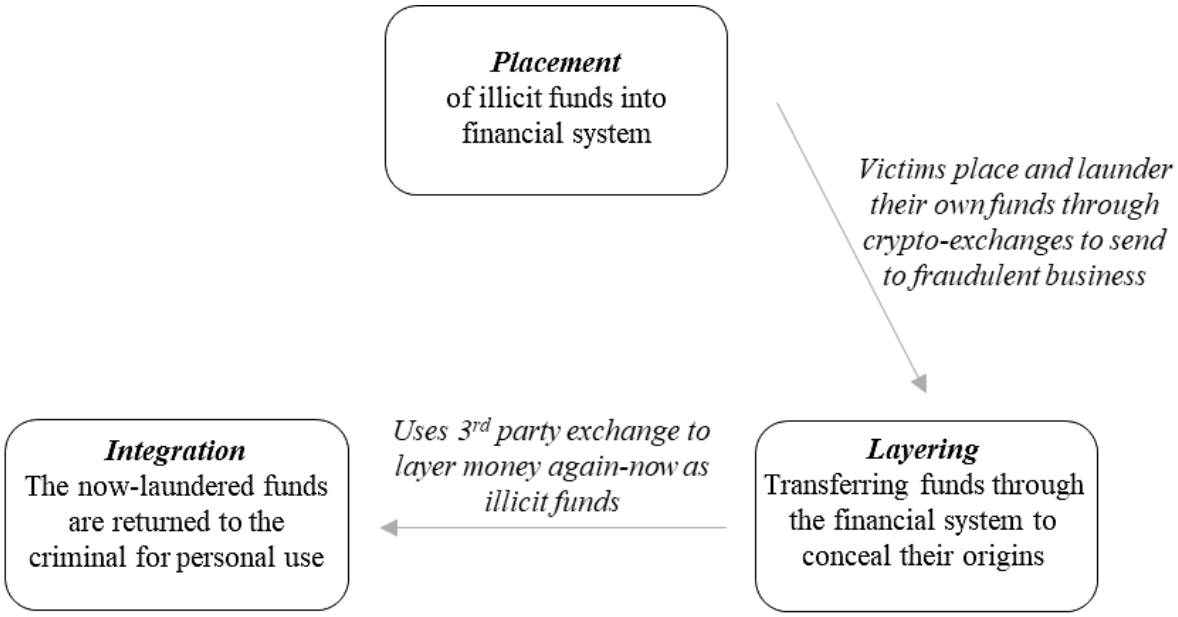


Figure 3 Crypto Laundering Process

Organizations deploy and improve system-based prevention mechanisms leveraging RegTech (Ruiz & Angelis, 2021) in an effort to reduce crypto laundering. RegTech, as the term suggests that is an information technology with the means to assist and support organizations prepare for compliance with lawful obligations and it holds a promise of solutions that will be reliable, safe, and more economical (Zabelina et al., 2018). Anagnostopoulos (2018) describes how RegTech focuses on streams in lowering the compliance burden and streamlining overall organizational performance. The use of RegTech for the prevention of crypto laundering is based on the assumption that it increases the capacities of institutions and regulators to combat financial crime (Kurum, 2020) through data analysis and on exchange of information that can improve risk mapping and support of investigations of the financial system (Zabelina et al., 2018). RegTech is rapidly evolving, which can be roughly segmented into three generations (KPMG, 2018): (1) RegTech 1.0 began in 1990s to 2000s before the global crisis occurred in 2008, which addressed risk assessment; (2) RegTech 2.0 initiated in the 2010s and concentrated on Know Your Customer (KYC) for Anti-Money Laundering (AML) compliance; and (3) RegTech 3.0 initiated in the 2019s and emphasized the Know Your Data (KYD) in Financial Crimes Compliance (FCC) through data analytics to predict potential risks (Teichmann et al., 2022). RegTech leverages big data and cloud technology to collect and store huge data sets of data that are not structured (i.e., too many variables, too many data points), which allows the process of analyzing and exchanging data quickly and accurately. According to literature review RegTech also assists organizations for automate reporting and abnormal activity identification (Zabelina et al., 2018). Table 2 explains how RegTech assists enterprises in implementing crypto money laundering prevention.

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)

The prevention technology based on regulations (RegTech) should be supplemented with the direct monitoring of the financial system to establish an integral action against crypto laundering to decrease its systemic risk that could hurt international stability of financial and economic systems (Reznik et al., 2021). Financial control in the economic aspect of a country should also be equipped with financial monitoring. The proper financial control can be implemented from financial intelligence point of view through the applying specific methodology of control presented in the Table 3 (Reznik et al., 2021).

Table 3 Scope of Financial Intelligence

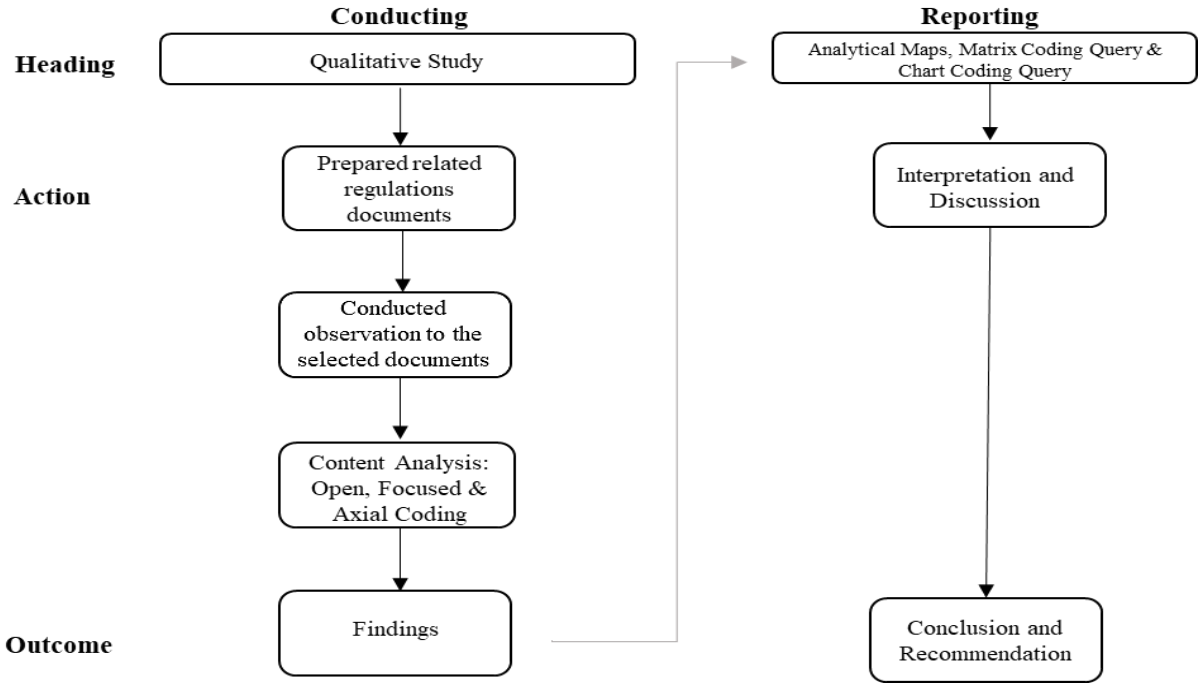
Controller	Controlled	Controlled Object	Purpose
Institutions with financial control functions designated by the state	All types of business entities, institutions, organizations, and individuals	Legality, use, reliability, and economic efficiency of financial activities	Prevent transactions that may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

The application of financial intelligence is in the control of the institution appointed and established by the state (controller). Although the name of the institution may vary from one country to another, it is generally called the Financial Intelligence Unit (FIU) (Reznik et al, 2021), and the FIU usually plays the role of the AML coordinator in the country (Sultana, 2020; Naheem, 2018). The primary role or in-house role performed by FIU is to share, scrutinize and disseminate (Reznik et al., 2021) reports about entities or individuals the it believes that there exists suspicious of SAR of financial activity (Sultana, 2020) on the basis of certain indicators and applicable regulations (Williams, 2014). Simultaneously, on the external function, that is the FIU cooperating with other countries' FIUs, providing efficiency to the prevention of crypto laundering on an international scale (Williams, 2014). Based on FATF (2003), FIU has a role in carrying out the exchange of information from one to another country (FIU to FIU) through the application of an open database based on bilateral or multilateral agreements of each country that exchanges information between FIU to FIU.

RESEARCH METHOD

In this paper we present system based (RegTech based) crypto laundering preventing mechanism within Indonesia based on the regulation rules that have been made and published by Commodity Futures Trading Regulatory Agency. This study used a qualitative study (Saunders et al., 2012), which was drawn from secondary data. The secondary analysis is a more profound investigation of the data in order to extract

knowledge, interpretation and conclusion that are different from previous findings (Bulmer et al., 2009). Figure 4 shows the research protocol conducted in this study.



The secondary data used in this study are presented in 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 Crypto Assets on the Futures Exchange
3	Head of CFTR Regulations and Attachment Number 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 Number 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

In addition, data were coded through qualitative content analysis or a coding process aimed at data reduction based on a priori categories (Molinari & de Villiers, 2021), which were analyzed using a content analysis approach (Holsti, 1969). The secondary data coding carried out using NVivo with three coding stages as follows: 1) Open coding (Corbin & Strauss, 2008) is an initial data analysis with organization of categorization of focus and simplification of data structure; 2) Focused coding (Charmaz, 2006), reviewing of data re-analysis—in the open coding stage—to group into significant categories; and 3) Axial coding (Corbin & Strauss, 2008) to find the relationship between significant data categories is a theoretical development process.

Authors use 'Qualitative Content Analysis' — a data analysis technique ' in Shi et al. (2022) and Silva (2022). Shi et al. 1 combined the techniques of two studies, where the authors. Silva (2022) performed open coding and axial coding to realize data reduction in his qualitative content analysis approach, and Alibaba (2022) used NVivo to help them in conducting qualitative content analysis. As a codification technique, the authors used

focused coding (Charmaz, 2006), to offer a web of complementary systematic information on results of data analysis (Saunders et al., 2012).

RESULT AND DISCUSSION

Meanwhile, the prevention of crypto laundering is regulated, established, and overseen by the CFTR, since the banking sector and all crypto asset trading activities are regulated by the CFTR/CFTR. Data analysis CFTR which states that prevention of crypto laundering in Indonesia is held up with Know Your Customer (KYC) and transaction monitoring with risk-based and RegTech-based. Crypto asset trading platform operators (crypto FinTech) particularly report to the Indonesian Transaction Report and Analysis Center (INTRAC), which functions as the FIU, for transaction monitoring activity. Results were also derived through analytical maps in order to clearly show the relationship of each finding as well as matrix and chart coding queries to demonstrate the volume of total coding processed from data sources. The appendix at the end of this article shows a visualization of the data.

RegTech For Crypto Money Laundering Prevention

Today, cryptocurrency is growing2 at the global level; a significant concentration of countries is becoming a major place for virtual asset exchanges (Kirkpatrick et al., 2021) including the United States, United Kingdom, Germany, Australia, and Japan. the number of virtual asset (crypto) customers has steadily risen for the last three years. (Tempo, 2023), at the end of October 2023 crypto asset customers numbered 18.06 million with a transaction value of IDR 104.9 trillion. Therefore, regulation of virtual assets is a very thing for regulators because it falls into the category of the riskiest investment instruments (Kirkpatrick et al., 2021), both the risk of loss that is a threat to investors and the risk of money laundering that is a threat to the law.

Overall, the relevant regulation in Indonesia underlies the process of stopping crypto laundering described by this study. The regulation concerning the use of virtual assets (crypto) and the process for preventing crypto laundering, sourced from NVivo 12–based content analysis, is shown in Table 5. This code assigned in Table 5 relates to results of data analysis which is included

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	a. Risk mapping
	b. Risk tolerance	b. Establishment of risk limits
	c. Risk reduction and control	c. Internal control and risk mitigation
	d. Risk residual evaluation	d. Ensuring the residual risk level is not higher than the risk tolerance
	e. Implementation of a risk-based approach	e. Risk-based approach cycle documentation
	f. Risk-based approach review and evaluation	f. The effectiveness assessment of crypto laundering prevention program implementation
Know Your Customer (KYC) Due Diligence	• Based on a risk-based approach	
Customer Enhanced Due Diligence	• RegTech-based with face recognition features and liveliness characteristics	

	• Data identification and verification integrated with the Ministry of Home Affairs' biometric data	
Transaction Monitoring	• Implement the Know Your Transaction (KYT)	
	• Verification of withdrawals or transfers	
	• Using blockchain analytic tools	

Source: NVivo 12, Processed (2023)

the copulation of virtual assets (crypto) is only from trade in futures exchanges, and not a medium exchange. This is consistent with the regulations in Germany where the use of the algorithm is limited to the scenario mentioned above. For example, Germany allows crypto assets to be used only for trading, and they are not treated as a medium of exchange (Kirkpatrick et al., 2021). The Federal Financial Supervisory Authority is the central regulator and thus responsible for the regulation of crypto asset trading in Germany. Similarly, in the UK and Japan, regulation of virtual asset trading is in the jurisdiction of the Financial Conduct Authority (FCA) and Japan's Financial Service Authority (JFSA) respectively.

This study confirmed that the regulation of virtual asset trading remains in force in accordance with the power and jurisdiction of CFTR (Commodity Futures Exchanges Regulatory Agency). Taking a cue from Germany, UK and Japan, virtual asset trading regulation concept in Indonesia ought to be a duty and responsibility from the Financial Service Authority (Otoritas Jasa Keuangan). FSA also has a role to simplify an integrated regulatory and supervisory system for all financial activities in the financial services sector to ensure that all activities on virtual asset (crypto) trading shall be supervised and regulated by FSA. On the prevention of money laundering of virtual asset, the finding showed that the prevention process that occurs in Indonesia is by way of conducting KYC (Know Your Customer) and transaction monitoring.

The study has found that organizations in the implementation of KYC activities utilize face recognition technology with liveliness characteristics and RegTech based technology integrated with biometric data or population administer data owned by the Ministry of Home of Affairs. This result is in line with prior literature where studies show that the use of RegTech in the KYC procedure is essential in order to hinder financial crime (Kurum, 2020). Yet the use of face recognition using biometric data poses further complexity regarding data privacy. The study designed by Liyanaarachchi et al. (2023) discovered that the collection of biometric data has negative effects on individuals because this reduces the individuals control to their person data as well as transferring the control of the way that the people use their data back to organization The integration of biometric data collected by organizations with the Ministry of Home Affairs' biometric data does not translate to the legality and freedom from issues of privacy imbalance (Liyanaarachchi et al., 2023). Instead, it portends new privacy issues. The access to data belonging to the Ministry of Home Affairs given to organizations is very likely to result in the Ministry of Home Affairs violating the ethical guidelines on the use of privacy-oriented technology (Ryan & Stahl, 2021). Regulators should thus review and define regulations and guidelines for data collection as part of the KYC process that could give more confidence to the individuals that the data collection is being done within ethical, security and data privacy guidelines. It is also to prevent collection of massive, meaningless, false, and unrelated data (Sarabdeen, 2023). Technological Acceptance Model (TAM) should be extended to incorporate legal and regulatory considerations as integral components of data privacy (Akanfe et al., 2024).

On the other hand, while companies conduct transaction monitoring, organizations must use blockchain analytic tools since transactions related to crypto assets are in a decentralized manner with the support of blockchain technology. In line with Bhatt et al. (2020) that the use of blockchain technology with other technologies, e.g., artificial intelligence (AI), had advantages and investment in blockchain technology. Based on regulations, the authors did not discover much about the mechanism used in blockchain analytic tools. However, it must be that

the mechanism should be able to analyze the consensus algorithms mechanism, the core (Bamakan et al., 2021). The key consensus algorithms in blockchain technology are proof of work, proof of stake, and proof of elapsed time (Bamakan et al., 2020). These three consensus algorithms are integrated into the chain of transaction blocks on the blockchain as they serve the functions of transaction verification, reading the quantity of mine wealth as well as transaction security. So, the authors would like to expect blockchain analytic tools that are regulated in Indonesia utilize those three consensus algorithms as the basis to analyze and define the anomalous crypto asset transaction that happened on the blockchain, also the blockchain address that has the transaction.

Blockchain is a disruptive technology; according to Bamakan et al. (2021), there has been a challenge regarding energy consumption by blockchain, that is, blockchain consumes a notable amount of energy so blockchain exhaust the energy sources. Therefore, regulators need to work with experts to review how reality blockchain technology really affects energy resources and then begin to consider regulating renewable energy in an environmentally friendly way in order to avoid the impact of environmental degradation is a disruption of sustainable development.

Rule-based system policy: KYC and transaction monitoring procedures based through regulations need to be implemented by referring(youring) risk-based approach policy, so crypto FinTechs need to perform a risk assessment. This outcome is consistent with the results from the crypto laundering prevention process in other countries including the UK and Bermuda (Kirkpatrick et al., 2021). Generally, there are applicable regulations from Indonesia, the UK, and Bermuda on the prevention of crypto laundering which must be formalized within the process of risk assessment, KYC, and transaction monitoring. However, if you are comparing specifically, the regulation of those three countries is different.

In the UK, education and training of human resources (HR) involved directly in preventing the laundering of cryptocurrencies is a component of the regulation of mechanisms preventing the laundering of cryptocurrencies (Kirkpatrick et al., 2021). In Indonesia, though, it has yet to be included in the regulation. As of now, crypto laundering prevention has it technically regulated on the system, but there has not yet been regulations for human resources. This regulation merely governs the criteria that must be met in order to select the HR through the KYE (Know Your Employee) process before the HR takes any action towards the organization. The low Arte & awareness of crypto laundering risk for the crypto FinTech reflects the absence of role of regulations and regulators in HR management.

In contrast, regulations in Bermuda mandate organizations to periodically test their crypto laundering prevention procedures for relevance and adequacy in addressing any issues (Kirkpatrick et al., 2021). this is not regulated. Failure with regard to inclusion of provisions on periodic review examination is a weakness that works against the enforcement of crypto laundering preventing regulations. Implementation of the relevant regulations in the UK and Bermuda can be drawn consideration for the relevant regulators and parties that the current regulations applicable in Indonesia still need to be reviewed and re-optimized because created regulations must ensure that all elements that prevent crypto laundering can be reached and can predict future-possible events (McCarthy, 2022).

The Role of Financial Intelligence Units in Crypto Laundering Prevention

The Financial Intelligence Unit (FIU) is responsible for the gathering, analyzing, and distribution of reports which would signify suspicious financial activity on behalf of the entities or individuals (Reznik et al., 2021) in question (Sultana, 2020). The research results state that this role is performed by the Indonesia Transaction and Report and Analysis Center (INTRAC) as an independent NOTP institution that has the task of preventing and eradicating all forms of money laundering in cooperation with other parties (anti-money laundering regime) and forwarding the results of its analysis to law enforcement agencies. According to an analysis of various biorational FIU of Western countries (Canada, Denmark, Netherlands, Luxemburg, United States) and of Eastern countries (Estonia, Latvia, Lithuania, Poland, Ukraine), FIU is based on a national institution which is not homogeneous (McNaughton, 2023). The reasons are that (i) on normative level the subject of FIU activity is governed by the respective national AML framework. The study's findings suggest the degree of the FIU's role varies from country to country. According to McNaughton (2023) countries have accordingly set up FIUs usually following

either an administrative or a law enforcement-based model. In the administrative model, the functions performed by the FIU actually yield the information required (tactics intelligence) for the investigators or law enforcement, and act as a supervisory authority to ensure the AML compliance from reporting parties or financial institutions. FIU in this model has no authority power to conduct investigations. While in law enforcement model FIU has authority to investigate, seize suspicious transaction and execute law. A special police unit is usually granted this type of model. However, a few countries establish a third type of FIU known as a judicial FIU, which is a specialized unit within the Attorney General's Office and incorporates the characteristics of the administrative and law enforcement type FIU.

This study finds no evidence that Indonesia uses any of the four FIU models. INTRAC's role and authority does not cover oversight of compliance functions and law enforcement, and INTRAC is neither under the Attorney General's Office nor a specialized unit in the police. INTRAC is independent and reports directly to the president, making periodic reports on its exercise of its authority to the president and the House of Representatives. Nevertheless, across the FIU models there are no general provisions that should apply to any country, or FIU for that matter. The FIU model adopted is the normative basis of the AML framework.

The research findings reveal that INTRAC has the assignment and authority to receive the reports from crypto FinTech on suspicious transaction on the basis of the results received by RegTech which refers to the application of blockchain analytic tool.

The insights contained in the report stem from the combination of blockchain - the technology that underpins crypto asset exchange - with artificial intelligence (AI) through blockchain analytic tools. The simulation results of the Integrated Blockchain and Artificial Intelligence Framework (IBAI Framework) confirm this finding. An Algorithmic Framework proposed by Alenizi et al. (2024) and rehearsed the financial transactions. According to the simulation, there are substantial numerical outputs that the IBAI Framework shows promising numerical performances that will upsurge the detection ratio of the suspicious behaviors with an accuracy rate of 98%. The effective optimization of the application of blockchain analytic tolls will ultimately have a positive impact on the integrity of reports received by INTRAC so that, ideally, it can facilitate INTRAC in carrying out its role to carry out further analysis of suspicious transactions. According to the findings, INTRAC conducts further analysis using a follow-the-money approach and sends the results of their analysis to law enforcement agencies. However, when it comes to the impact of electronic money laundering/crypto laundering their operations could be a challenge for FIUs in developing countries in engaging further into electronic money laundering results from other developing countries like Tanzania, due to limited tools and technology available to FIUs to engage into further analysis for suspicious transaction in blockchain (Mniwasa, 2019). Because of the fact it is a developing country, and suffers from the same responsible for preventing and eradicating all types of money laundering, so that can have an impact on the continued presence of INTRAC. Thus, it is the responsibility of the regulators/AML regimes to ensure the same INTRAC has the sufficient tools and technology to conduct analysis of some transaction type with the underlying technologies used. Similarly, the human resources assigned must be performed by people with the necessary qualifications and expertise. Tools, technology and human resources as a representation of INTRAC must correlate with the other the existence of INTRAC in carrying out its authority that can weaken or strengthen the role of INTRAC as FIU.

CONCLUSION

The mechanism documented by this study outlines how CFTR acts to restrict crypto laundering. In general terms, crypto laundering prevention measures include Know Your Customer (KYC) and transaction monitoring procedures, which take place on a risk-based approach. In normative terms, this prevention mechanism is used in RegTech via face recognition for KYC and blockchain analytic tools for transaction monitoring. The application of RegTech in Indonesia is implemented on an ongoing basis with the INTRAC's role as the Financial Intelligence Unit (FIU). INTRAC is an independent, direct reporting unit to the president. This indicates that INTRAC is entitled to receive suspicious transaction reports from financial entities and has the power to analyze such transactions. INTRAC's ability to analyze suspicious transactions related to crypto assets relies on the capacities of its tool, technology, and human resources capabilities. These three aspects are crucial

for INTRAC to ensure the continuity of its functions as FIU and part of the AMLC in Indonesia. In this case, Indonesia must firmly position the FIU to become a responsive and adaptive actor to the dynamics of financial technology developments in order to avoid the misuse of financial technology as a means of laundering crypto-assets.

They draw attention to the crypto laundering prevention mechanism and the role of the FIU that have not been comprehensively established to provide theoretical insights and practical implications, advocating the Commodity Futures Trading Regulatory Agency and the Financial Service Authority as the stakeholders re-examine and develop the crypto laundering prevention mechanism based on its underlying technologies, as well as the parties of the anti-money laundering regime to collaborate with experts from various fields.

This study has been performed and oversighted pragmatically. Still, the authors admit, there are things that they cannot control and can be a future research opportunity. This research is also limited because of its reliance on the study of secondary data (regulatory documents) that still has to be optimized by offering the explanation of the entire RegTech and FIU mechanism. This did, however, mean that RegTech and FIU's role were only examined normatively. Future studies are likely to elaborate on how the role of RegTech and FIU has been functioning in keeping crypto laundering at bay empirically and compare the empirical results vis-a-vis the normative prescriptions in this study.

REFERENCES

1. Adachi, D., & Aoyagi, J. (2020). Blockchain and Economic Transactions. Cryptocurrency and Blockchain Technology. https://doi.org/10.1515/9783110660807-002
2. 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
3. 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
4. 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-072022-0109
5. 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
6. Albrecht, W., Albrecht, C., Albrecht, C., & Zimbelman, M. (2012). Fraud Examination (4th ed.). Cengage Learning South-Western.
7. 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
8. 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
9. 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
10. 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.
11. 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.
12. Bulmer, M., Sturgis, P. J., & Allum, N. (2009). Secondary Analysis of Survey Data. SAGE.
13. Bylund, A. (2023). What Is Blockchain? The Motley Fool. https://www.fool.com/terms/b/blockchain/

14. Chainalysis. (2022). The 2022 Crypto Crime Report (Issue February). https://go.chainalysis.com/2022-crypto-crime-report.html
15. Charmaz, K. (2006). Constructing Grounded Theory. In British Library. SAGE.
16. Corbin, J., & Strauss, A. (2008). Basics of Qualitative Research (3rd ed.). SAGE.
17. Dyntu, V., & Dykyi, O. (2019). Cryptocurrency in the System of Money Laundering. Baltic Journal of Economic Studies, 4(5), 75–81. https://doi.org/10.30525/2256-0742/2018-4-575-81
18. FATF. (2003). The Forty Recommendations.
19. FATF. (2022). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF, Paris, France, March, 1–142. www.fatfgafi.org/recommendations.html
20. Finder. (2022). Finder Cryptocurrency Adoption Index. https://www.finder.com/id/findercryptocurrency-adoption-index
21. Gottschalk, P. (2010). Categories of financial crime. Journal of Financial Crime, 17(4), 441–458. https://doi.org/10.1108/13590791011082797
22. Holsti, O. (1969). Content Analysis for the Social Sciences. Addison-Wesley.
23. 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.
24. https://www.who.int/news-room/fact-sheets/detail/autism-spectrum-disorders
25. 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
26. Kementerian Keuangan RI. (2022). Menuju Era Uang Rupiah Digital. https://djpb.kemenkeu.go.id/portal/id/berita/lainnya/opini/3950-menuju-era-uangrupiah-digital.html
27. 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
28. 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-revolutioncoming.pdf
29. 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
30. 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
31. Litchfield, H. (2015). A Novel Method for Decentralized Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology. Australian Computer Society.
32. 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/IJCHM06-2023-0861
33. 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
34. Mardiansyah. (2021). Penilaian Rissik Indonesia Pencucian Uang. Pusat Pelaporan dan Analisis Transaksi Keuangan.
35. 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
36. 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
37. 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/JMLC04-2022-0059
38. 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

39. Molinari, M., & de Villiers, C. (2021). Qualitative accounting research in the time of COVID19 – changes, challenges and opportunities. Pacific Accounting Review, 33(5), 568–577. https://doi.org/10.1108/PAR-09-2020-0176
40. Moore, M. (2018). Everything You Need to Know About Blockchain. Albawaba.https://www.albawaba.net/business/everything-you-need-know-about-blockchain1158228
41. 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
42. 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/JFC10-2016-0064
43. Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 5: Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka, (2019).
44. Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka, (2021).
45. Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 11 Lampiran: Pedoman Penerapam Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme pada Pialang Berjangka, (2017).
46. Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme pada Pialang Berjangka, (2017).
47. 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).
48. Pickett, K. H. S., & Pickett, J. (2002). Financial Crime Investigation and Control. Wiley.
49. 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
50. 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
51. 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-09-20210106
52. 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-122019-0138
53. 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/IJLMA03-2023-0042
54. Sauners, 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.
55. 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
56. 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
57. 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
58. 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

59. 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
60. 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
61. Tempo. (2023). Tren Investor Aset Kripto Meningkat Sepanjang 2023, tapi Nilai Transaksi Menurun. https://bisnis.tempo.co/read/1805369/tren-investor-aset-kripto-meningkatsepanjang-2023-tapi-nilai-transaksi-menurun
62. 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
63. 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
64. 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/JFC11-2016-0067
65. 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
66. 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
67. 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-042021-0035
68. 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
69. Zabelina, Vasiliev, & Galushkin. (2018). Regulatory Technologies in the AML/CFT. KnE Social Sciences, 3(2), 394. https://doi.org/10.18502/kss.v3i2.1569
70. 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
71. Larkin, S. B. (2025). Lipstick on a Slaughtered Piggybank: Civil RICO Against "Pig Butchering" Cryptocurrency Investment Schemes. Roger Williams University Law Review, 30(1), 2.