

Preventing Crypto-Laundering through Regulatory Technology (RegTech): A Guiding Framework for Evaluation Studies in Indonesia

Kharisma Fatmalina Fajri^{1*}, Dekar Urumsah²

¹Accounting, Faculty of Business and Economics, Universitas Islam Indonesia, Indonesia

²Accounting, Faculty of Business and Economics, Universitas Islam Indonesia, Indonesia

*Corresponding Author: kharisaffajri@gmail.com

ABSTRACT

In Indonesia, the use of RegTech in preventing crypto-laundering is still developing. However, its effectiveness has not shown significant results, so exploration is needed into the cause of the ineffective use of RegTech. This study aims to propose a guiding framework for the evaluation of the use of RegTech. Data were obtained from various journal databases and then reviewed through a literature review with researchers as the research instrument. The guiding framework resulting from this literature review is expected to provide guidance for further researchers and stakeholders in evaluating the use of RegTech in preventing crypto-laundering in Indonesia.

Keywords: Crypto-Laundering, Crypto-Laundering Prevention, Regulatory Technology

INTRODUCTION

Cryptocurrency is a form of virtual currency that was created with the aim to speed up and cheapen the transaction process and is reliable when compared to the currency issued by the central bank or monetary authority of a country (Hossain, 2021). This currency is intangible (Adachi & Aoyagi, 2020) and uses encryption techniques to verify the transfer of funds (Hossain, 2021) through the blockchain (Litchfield, 2015). The use of cryptocurrencies is increasing significantly with the total transaction volume reaching USD 15.8 Trillion in 2021 or an increase of 567% from the total amount in 2020 (Chainalysis, 2022). With such developments, it is not surprising that cryptocurrencies are widely used by cybercriminals (Chainalysis, 2022).

The largest use of cryptocurrency in financial crime activities is used by perpetrators in money laundering or ML activities with a total of USD 33 billion from 2017 to 2021 (Chainalysis, 2022). In 2021 alone, the use of cryptocurrency in ML or crypto-laundering activities increased by 30% (Chainalysis, 2022). Perpetrators relatively use cryptocurrency in ML activities in order to avoid and not be easily detected by law enforcement officials (Wronka, 2022a; Wronka, 2022b; Mardiansyah, 2021) because transactions through cryptocurrency are relatively anonymous and difficult to identify (van Wegberg et al., 2018; Albrecht et al., 2019; Leuprecht et al., 2022; Al-Tawil, 2022). The use of cryptocurrencies does not stand alone, usually the perpetrators use cryptocurrencies at the placement and transfer stages (layering), then integrated with the use of legal currencies (fiat currencies) at the integration stage (Leuprecht et al., 2022). This use of multiple currencies makes crypto-laundering activities more difficult to detect (van Wegberg et al., 2018; Leuprecht et al., 2022).

Therefore, risk mitigation and crypto-laundering prevention efforts need to be effectively implemented by each virtual asset service provider whose compliance is overseen by local monetary authorities (FATF, 2022). However, compliance by virtual asset service providers with local country regulations as well as reporting to local monetary authorities of suspicious transactions is becoming more costly and complicated due to the large proliferation of data generated from cryptocurrency transaction activity (Teichmann et al., 2022). The emergence of regulatory technology or RegTech is a new technology as a solution that can support the compliance function of an organisation (Freij, 2020; Singh et al., 2022). In crypto-laundering, RegTech supports the compliance function of virtual asset service providers with regulations set by authorised institutions as an effort to prevent crypto-laundering (Teichmann et al., 2022). Some of the technologies used in RegTech are proven to help control and analyse transactions and verify identity quickly and accurately (Zabelina et al., 2018), including machine learning (Ruiz & Angelis, 2021), artificial intelligence (Kurum, 2020), and cloud computing (Kurum, 2020).

Several studies on crypto-laundering (Leuprecht et al., 2022; Wronka, 2022c; Akartuna et al., 2022; Albrecht et al., 2019; Dyntu & Dykyi, 2019; van Wegberg et al., 2018) and RegTech utilisation (Utami & Septivani, 2022b; Utami & Septivani, 2022a; Singh et al., 2022; Meiryani et al., 2022; Singh & Lin, 2021; Kurum, 2020; Naheem, 2018; Anagnostopoulos, 2018) have been conducted. Meanwhile,

research that specifically describes the use of RegTech in preventing crypto-laundering is only conducted by Ruiz & Angelis (2021). As for Indonesia, the use of RegTech in preventing crypto-laundering is still growing (Financial Services Authority, 2022). However, its effectiveness has not yet shown significant results (Utami & Septivani, 2022a; Utami & Septivani, 2022b; Meiryani et al., 2022), so it is necessary to explore the causes of the ineffective utilisation of RegTech. Therefore, this research aims to propose a guiding framework in conducting an evaluation study on the utilisation of RegTech in preventing crypto-laundering in Indonesia.

THEORETICAL STUDIES

Money Laundering

The term "Money Laundering" was first used in the 1930s by the American mafia who set up 'laundering' facilities to legitimise their criminal proceeds (Schneider & Windischbauer, 2008). Money laundering (ML) is one of the sub-categories of financial crime and is an important activity for most criminals because ML has a motive to gain economic benefits from several illegal activities, such as: embezzlement, fraud, misappropriation, corruption, robbery, distribution of narcotic drugs and human trafficking (Gottschalk, 2010; Lukito, 2016). The worldwide increase in drug trafficking, corruption and organised crime has increased the propensity of perpetrators to launder proceeds derived from their illegal activities (Fabre, 2003). In general, ML can be said to be the process of hiding the proceeds of crime or illegal origin and transforming them into legal and legitimate assets (CAMS, 2012). The ML process is divided into three stages called the three-stage process (Gottschalk, 2010), namely:

- a. Placement Stage, moving funds that originate and are directly related to criminal activity;
- b. Layering Stage, disguising traces to make it difficult for the authorities to detect;
- c. Integration Stage, legitimising the proceeds so that they can be freely used by the perpetrator for personal gain by purchasing assets or investing in legitimate businesses.

Crypto-Laundering

In 2009, Satoshi Nakamoto created bitcoin, which was the beginning of the introduction of virtual currency or cryptocurrency (Albrecht et al., 2019). In its early days, cryptocurrency was considered a low risk to engage in ML activities. However, as the use of cryptocurrencies has increased, the number of reports of suspicious transaction activity related to crypto-laundering has also increased (Wronka, 2022c).

Transactions through cryptocurrencies are based on blockchain technology so that each transaction is recorded in a public distributed ledger in chronological order. Given the inherent nature of such technology (Hossain, 2021) and the stateless nature of cryptocurrencies, this allows parties to conduct transactions directly around the world without involving intermediary financial institutions (Hossain, 2021). However, the owners of these transactions are difficult to identify

due to their relative anonymity (Albrecht et al., 2019; Leuprecht et al., 2022). There are three characteristics of cryptocurrencies that cause them to be used in ML activities (Wronka, 2022c):

- a. Anonymity or Pseudonymity. Cryptocurrency is a currency with a high level of anonymity when compared to fiat currencies. This is because the perpetrators can make changes to the crypto account address by having several public keys in one account, making it difficult to trace ownership.
- b. Low Barriers to Entry. With its decentralised and anonymous nature, opening a crypto account requires relatively fewer requirements for identification of potential customers when compared to opening a conventional bank account. In addition, transactions carried out in the cryptocurrency trading ecosystem also do not rely on intermediary institutions so that transactions can be carried out directly and privately which makes it difficult to detect if there are suspicious transactions.
- c. Global Tradability. Cryptocurrency trading is not limited by countries due to its virtual nature so that cryptocurrency exchanges only require an internet connection, not requiring various processes and approvals from intermediary institutions.

The crypto-laundering process consists of three main stages, which are as follows:

- a. Placement. This stage is very important (Albrecht et al., 2019) because the perpetrators exchange fiat currencies derived from illegal acts with cryptocurrencies (Wronka, 2022c) to be placed in the perpetrator's wallet.
- b. Layering (Transfer). Perpetrators typically use cryptocurrencies - previously derived from fiat currencies - for trading, investing or exchanging coins with other cryptocurrencies in different jurisdictions due to their virtual and stateless nature (Leuprecht et al., 2022).
- c. Integration. At this stage, actors exchange cyptocurrency with fiat currency (Leuprecht et al., 2022; Albrecht et al., 2019) so that it can be used in a legitimate monetary cycle (Wronka, 2022c).

Regulatory Technology (RegTech)

Regulatory Technology (RegTech) is an information technology (Zabelina et al., 2018) created as a solution to support the compliance function through internal process efficiency (Freij, 2020; Anagnostopoulos, 2018), collaboration with regulators for reporting, and system integration and simplification (Freij, 2020). Since the 1990s until today, RegTech has undergone a development that is divided into three phases (KPMG, 2018), namely: (1) RegTech 1.0 focused on risk assessment starting in the 1990s until the 2000s before the global crisis in 2008; (2) RegTech 2.0 focused on know your customer (KYC) for AML compliance starting in the 2010s or after the financial crisis; and (3) RegTech 3.0 focused on know your data (KYD) in financial crime compliance (FCC) using data analytics to estimate potential risks (Teichmann et al., 2022) starting in 2018.

In the prevention of crypto-laundering, RegTech is a tool to enhance the capabilities of institutions and regulators (Kurum, 2020) through optimising risk mapping, data analysis, and information exchange (Zabelina et al., 2018). RegTech

uses big data and cloud technology to collect and store large amounts of unstructured data and uses artificial intelligence (Kurum, 2020) and machine learning (Ruiz & Angelis, 2021) in conducting data analysis so that the process of data analysis and information exchange can be done quickly and accurately. The utilisation of RegTech in preventing crypto-laundering is presented in Table 2.

Tabel 1. Peran RegTech dalam Pencegahan *Crypto-Laundering*

Pencegahan <i>Crypto-Laundering</i>	Tujuan	Peran RegTech	Referensi
<i>Risk Assessment</i>	Mengidentifikasi dan meningkatkan pemahaman mengenai risiko ML pada organisasi	Digitalisasi sistem pengawasan untuk memetakan potensi risiko	Juntunen & Teittinen (2022); Zabelina <i>et al.</i> (2018)
<i>Electronic Know Your Customer (eKYC)</i>	Memeroleh informasi mengenai <i>customer</i> sebelum melakukan kerjasama	Digitalisasi pengumpulan informasi untuk meningkatkan akurasi dan reliabilitas dari informasi yang diperoleh	Juntunen & Teittinen (2022); Meiryani <i>et al.</i> (2022)
<i>Transaction Monitoring</i>	Mengawasi setiap transaksi yang dilakukan oleh <i>customer</i>	Identifikasi dan prediksi transaksi keuangan mencurigakan (<i>suspicious transaction</i>)	Akartuna <i>et al.</i> (2022); Meiryani <i>et al.</i> (2022)
<i>Cost and Time Efficiencies</i>	-	Mengakselerasi proses dan menurunkan biaya pencegahan ML	Meiryani <i>et al.</i> (2022)

Source: Researcher, Processed

RESEARCH METHODS

Formulation of Research Guideline Framework

This article proposes a guiding framework to explore the causes of ineffective utilisation of RegTech in preventing crypto-laundering in Indonesia. The formulation is conducted through a qualitative approach (Saunders *et al.*, 2012) sourced from secondary data. Secondary data in this formulation is obtained through published literature, in the form of journal articles and government

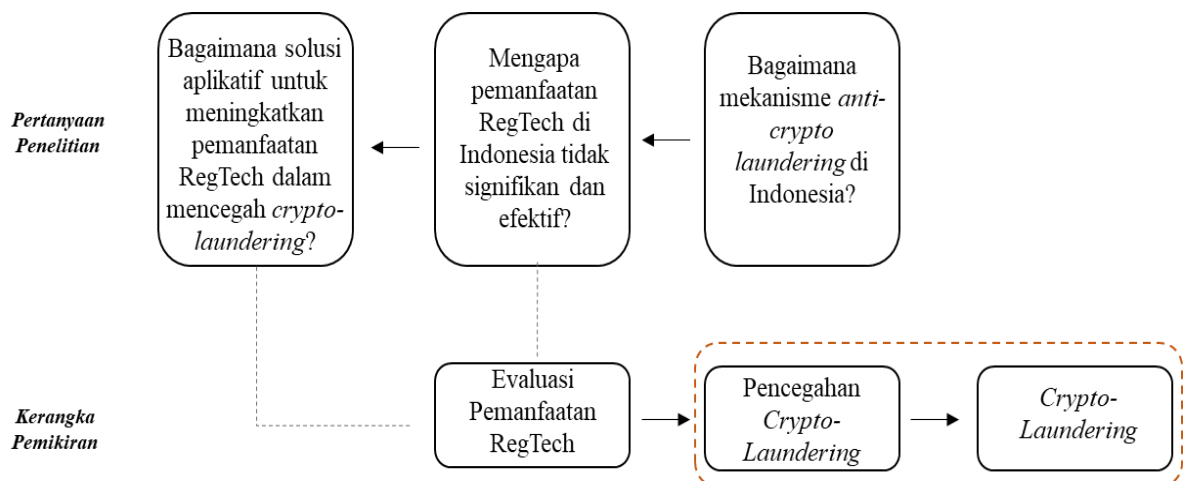
documents from various databases, such as: Emerald Database, Elsevier Database, and Google Scholar. The data focuses on crypto-laundering, anti-money laundering, anti-crypto laundering, and the utilisation of regulatory technology (RegTech).

Furthermore, data mapping is carried out through literature review to identify research gaps and theoretical foundations used so that researchers can determine research questions and determine the paradigm used to answer research questions. The research paradigm can assist researchers in gaining an understanding of the phenomena that occur (Saunders et al., 2012). Through this identification and understanding, researchers can formulate a research guideline framework to explore the causes of ineffective use of RegTech in preventing crypto-laundering in Indonesia.

RESULTS AND DISCUSSION

Research Guideline Framework

Based on the results of the literature review that has been carried out, it is known that the paradigm to be used in the research is the functionalist paradigm which is structured by the dimensions of objectivitis and regulation (Saunders et al., 2012). Research conducted based on the functionalist paradigm becomes an evaluation study to assess the effectiveness of a phenomenon and make recommendations to improve the effectiveness of the phenomenon (Saunders et al., 2012). Therefore, the research questions and framework proposed in the evaluation study on the ineffective utilisation of RegTech to prevent crypto-laundering are illustrated by the researcher through Scheme 1.



The proposed guideline framework has questions that begin with "how" and "why", requiring a qualitative approach to answer the problem formulation. Qualitative approaches help researchers to answer complex questions, such as:

Skema SEQ Skema * ARABIC 1. Pertanyaan Penelitian dan Kerangka Pemikiran

how and why the implementation of best practices succeeds or fails (Hamilton & Finley, 2020). Qualitative research relies heavily on reality reconstruction (Khalid, 2009) or social constructionism in answering research questions

(Saunders et al., 2012) so that data collection is carried out through interviews with individuals and focus groups, observation, ethnography and or several other approaches (Hamilton & Finley, 2020). These types of data collection are considered to be the media with the best credibility in understanding the phenomena thought by the data source (Hamilton & Finley, 2020).

The data collection that will be conducted is based on the proposed research questions and can answer the research questions. Each research question is aimed at achieving the research objectives with the data sources presented in Table 2.

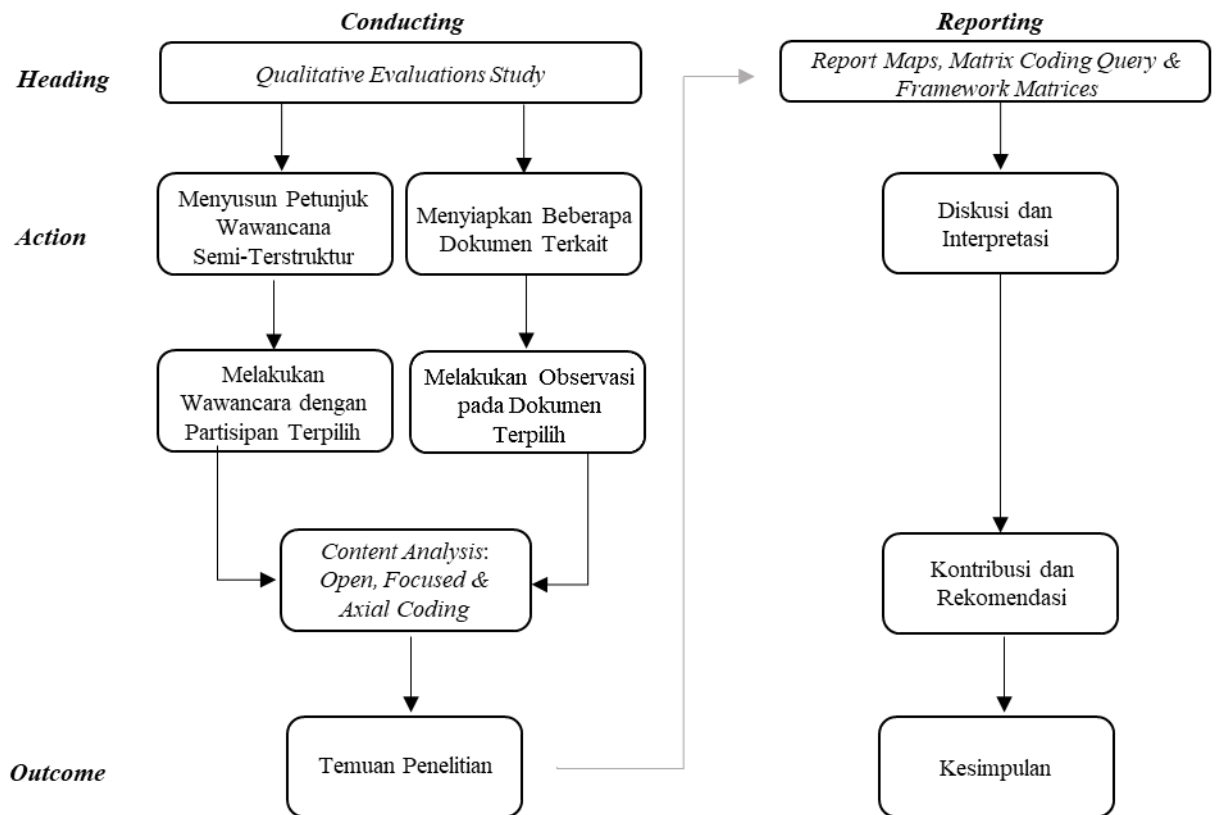
Tabel 2. Pertanyaan, Tujuan, dan Sumber Data Penelitian

No.	Pertanyaan Penelitian	Tujuan Penelitian	Sumber Data
1.	Bagaimana mekanisme <i>anti-crypto laundering</i> di Indonesia?	Mengetahui mekanisme, pedoman penerapan, dan pemanfaatan RegTech yang berlaku di Indonesia dalam mencegah <i>crypto-laundering</i> .	Data Sekunder: a. UU Nomor 7 Tahun 2011; b. Permendag Nomor 99 Tahun 2018; c. Peraturan Kepala Bappebti Nomor 8 tahun 2021; d. Peraturan Bappebti Nomor 5 Tahun 2019; e. Peraturan Bappebti Kepala Nomor 11 Tahun 2017; f. Peraturan Kepala Bappebti Nomor 8 Tahun 2017.
2.	Mengapa pemanfaatan RegTech di Indonesia tidak signifikan dan efektif?	Mengetahui penyebab tidak signifikan dan efektifnya pemanfaatan RegTech dalam mencegah <i>crypto-laundering</i> .	Data Primer: Wawancara semi-terstruktur dengan pihak-pihak yang memiliki pengetahuan mengenai <i>crypto-laundering</i> dan pemanfaatan RegTech di Indonesia, seperti: <i>Anti-Money Laundering Specialist</i> dan <i>Indonesian RegTech and LegalTech Association (IRLA)</i> .
3.	Bagaimana solusi aplikatif untuk menurunkan risiko penyebab dan tantangan dalam pemanfaatan RegTech untuk mencegah <i>crypto-laundering</i> ?	Memberikan rekomendasi perbaikan yang dapat digunakan oleh para pemangku kepentingan untuk meningkatkan pemanfaatan RegTech dalam mencegah <i>crypto-laundering</i> .	

Sumber: Peneliti, 2023

As illustrated in Scheme 1, all of the proposed research questions are intended as instruments in the evaluation of RegTech utilisation in Indonesia. The evaluation of RegTech utilisation aims to increase the effectiveness of the use of RegTech in preventing crypto-laundering because the utilisation of RegTech has been proven to increase the prevention of crypto-laundering (Ruiz & Angelis, 2021) so that the risk of crypto-laundering can decrease. Since the failure of money laundering and/or crypto-laundering prevention can have catastrophic consequences for the

victims (Truby, 2016), the details of the implementation process to answer the research questions - as presented in Scheme 1 - are presented in Scheme 2.



CONCLUSION

Based on the data analysis that has been conducted through the literature review, a guiding framework can be mapped out that aims to explore the causes of the insignificant and ineffective use of RegTech in preventing crypto-laundering in Indonesia. This guiding framework is detailed by the researcher in the form of research questions, framework, data required and the process of conducting research to answer the research questions. Each of these research questions is aimed at achieving the research objectives as well as being instrumental in the proposed evaluation study.

This guideline article has limitations in that the process of analysing the preparation of this evaluation guideline framework was carried out through literature review with the researcher as the research instrument so that the credibility, validity and significance of this guideline framework is based on the subjectivity of the researcher. This is because the researcher is not a neutral and objective observer so subjectivity is unavoidable in the process of developing the guideline framework for this evaluation.

REFERENSI

- Adachi, D., & Aoyagi, J. (2020). Blockchain and Economic Transactions. *Cryptocurrency and Blockchain Technology*. <https://doi.org/10.1515/9783110660807-002>
- 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, C., 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>
- 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>
- CAMS. (2012). *Certification Examination Certification Examination*. Association of Certified Anti-Money Laundering Specialists.
- Chainalysis. (2022). *The 2022 Crypto Crime Report* (Issue February). <https://go.chainalysis.com/2022-crypto-crime-report.html>
- 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>
- Fabre, G. (2003). Criminal Prosperity: Drug Trafficking, Money Laundering, and Financial Crises after the Cold War. *Psychology Press*.
- 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
- Freij, Å. (2020). Using technology to support financial services regulatory compliance: current applications and future prospects of regtech. *Journal of Investment Compliance*, 21(2/3), 181–190. <https://doi.org/10.1108/joic-10-2020-0033>
- Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime*, 17(4), 441–458. <https://doi.org/10.1108/13590791011082797>
- Hamilton, A. B., & Finley, E. P. (2020). Reprint of: Qualitative methods in implementation research: An introduction. *Psychiatry Research*, 283(August 2019), 112629. <https://doi.org/10.1016/j.psychres.2019.112629>
- Hossain, M. S. (2021). What do we know about cryptocurrency? Past, present, future. *China Finance Review International*, 11(4), 552–572. <https://doi.org/10.1108/CFRI-03-2020-0026>
- Juntunen, J., & Teittinen, H. (2022). Accountability in anti-money laundering – findings from the banking sector in Finland. *Journal of Money Laundering Control*. <https://doi.org/10.1108/JMLC-12-2021-0140>
- Khalid, S. N. A. (2009). Reflexivity in Qualitative Accounting Research. *Journal of Financial Reporting and Accounting*, 7(2), 81–95.

- <https://doi.org/10.1108/19852510980000005>
- KPMG. (2018). *There's a Revolution Coming: Embracing the Challenge of RegTech 3.0*. <https://assets.kpmg/content/dam/kpmg/uk/pdf/2018/09/regtech-revolution-coming.pdf>
- Kurum, E. (2020). RegTech solutions and AML compliance: what future for financial crime? *Journal of Financial Crime*. <https://doi.org/10.1108/JFC-04-2020-0051>
- Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*. <https://doi.org/10.1108/JFC-07-2022-0161>
- Litchfield, H. (2015). A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology. *Australian Computer Society*.
- 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.
- 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>
- 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>
- 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>
- Saunders, M., Lewis, P., & Thornhill, A. (2012). Research methods for business students. In *International Journal of the History of Sport* (Vol. 30, Issue 1). www.pearson.com/uk
- Schneider, F., & Windischbauer, U. (2008). Money laundering: Some facts. *European Journal of Law and Economics*, 26(3), 387–404. <https://doi.org/10.1007/s10657-008-9070-x>
- 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>

- 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>
- Truby, J. (2016). Qatar's progress towards preventing terror finance through the abuse of charitable status and the financial sector. *Journal of Money Laundering Control*, 19(4), 500–516. <https://doi.org/10.1108/JMLC-08-2015-0031>
- 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>
- 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>