RIGA GRADUATE SCHOOL OF LAW

Implementing Anti-Money Laundering Regulations in the Decentralized Cryptocurrency Industry: Challenges, Implications, and Solutions

MASTER THESIS

AUTHOR: Veronika Točilkina
LL.M 2022/2023 year student
student № M021012

SUPERVISOR: Paolo Paesani
PhD, Economics,
European University Institute Florence

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed) …….

RIGA, 2019

Abstract

This thesis examines the effective implementation of Anti-Money Laundering regulations in the decentralized and global cryptocurrency industry. It addresses the unique challenges posed by the decentralized nature of cryptocurrencies, such as anonymity, cross-border transactions, and lack of standardization, which create opportunities for financial crime. The study explores the regulatory landscape, including Anti-Money Laundering terminology, legal frameworks, and global cryptocurrency regulations. It also analyzes the practical implications of implementing Anti-Money Laundering regulations, focusing on the case of Dukascopy Bank's Dukascoin as a specific cryptocurrency example. The research highlights the need for clear and consistent regulatory guidance, technology-driven solutions, international cooperation, and risk-based approaches to combat financial crime. The findings contribute to the development of effective and coordinated approaches for addressing the risks of financial crime in the cryptocurrency industry.

Keywords: Anti-Money Laundering, cryptocurrency, decentralized, regulatory challenges, Dukascopy Bank, Dukascoin, technology-driven solutions, risk-based approach.

Summary

The cryptocurrency industry has experienced significant growth and popularity in recent years, along with concerns about money laundering and other financial crimes. This thesis focuses on the effective implementation of Anti-Money Laundering regulations in the decentralized and global cryptocurrency industry, taking into account its unique characteristics and challenges. Through an analysis of the legal aspects, practical implications, and case studies, this research provides valuable insights and recommendations for developing robust regulatory frameworks.

The thesis begins by examining the terminology and legal aspects related to Anti-Money Laundering regulation in the cryptocurrency field. It highlights the difficulties in regulating cryptocurrencies, including anonymity, cross-border transactions, lack of standardization, volatility, and regulatory arbitrage. Additionally, it explores global cryptocurrency regulations and the reasons behind the bans imposed by certain countries.

In the next section, the thesis focuses on the regulation of a specific cryptocurrency, Dukascoin, issued by Dukascopy Bank. It provides an overview of Dukascoin, its creation process, and implementation. The analysis also delves into the challenges faced by Dukascopy Bank from a legal perspective, offering insights into the practical implications of implementing Anti-Money Laundering regulations for a specific cryptocurrency.

The thesis further investigates current initiatives and potential improvements in cryptocurrency regulation. Stakeholders have suggested specific improvements, such as providing clearer and more consistent regulatory guidance. This includes guidance on custody requirements, Anti-Money Laundering compliance, and regulatory requirements for cryptocurrency exchanges. Additionally, the research reviews relevant case law, including the Tezos case and the Crypto AG case, to draw practical lessons and implications from real-world examples.

The findings of this research highlight the multifaceted nature of effectively implementing Anti-Money Laundering regulations in the cryptocurrency industry. It emphasizes the importance of technology-driven solutions, such as blockchain analytics, to enhance detection and prevention capabilities. The research also underscores the need for ongoing monitoring and adaptive regulatory frameworks to address evolving risks and challenges.

Moreover, the thesis emphasizes the significance of international cooperation and harmonization in combating financial crime in the cryptocurrency sector. It emphasizes the need for collaboration among regulators, international organizations, and industry associations to establish common standards and strategies. Additionally, the research underscores the value of public-private partnerships in fostering innovation, transparency, and responsible business practices.

The research presented in this thesis addresses two central research questions: how to effectively implement anti-Money Laundering regulations in the decentralized and global

cryptocurrency industry, considering its unique characteristics and challenges, and what are the practical implications and challenges of implementing anti-Money Laundering regulations in the cryptocurrency industry, as evidenced by the case of Dukascopy Bank's Dukascoin. By exploring these questions, this research offers valuable contributions to the field of cryptocurrency regulation and provides guidance for policymakers and stakeholders.

The first research question focuses on the effective implementation of Anti-Money Laundering regulations in the cryptocurrency industry. The analysis reveals that the decentralized and global nature of cryptocurrencies presents unique challenges for regulatory efforts. The inherent features of anonymity, cross-border transactions, lack of standardization, volatility, and regulatory arbitrage require innovative and adaptive regulatory approaches. The research emphasizes the importance of providing clear and consistent regulatory guidance tailored to the specific needs of the cryptocurrency industry. This includes specific guidelines on custody requirements, Anti-Money Laundering compliance, and regulatory requirements for cryptocurrency exchanges. By addressing these areas, regulators can enhance transparency, reduce ambiguity, and promote compliance in the industry.

Furthermore, the research highlights the significance of technology-driven solutions in combating financial crime in the cryptocurrency sector. The implementation of blockchain analytics and other advanced technologies can enhance the detection and prevention of money laundering and illicit activities. By leveraging these tools, regulators and law enforcement agencies can strengthen their investigative capabilities, monitor suspicious transactions, and identify potential risks in real-time. The research underscores the need for continuous investment in technological infrastructure and collaboration between regulatory bodies and technology providers to stay ahead of evolving threats in the cryptocurrency landscape.

The second research question examines the practical implications and challenges of implementing Anti-Money Laundering regulations in the cryptocurrency industry, using the case of Dukascopy Bank's Dukascoin as a specific example. The analysis sheds light on the complexities and considerations involved in creating and regulating a specific cryptocurrency. The case study of Dukascoin demonstrates the legal challenges faced by financial institutions when launching their own cryptocurrencies. It highlights the need for thorough due diligence, compliance with Anti-Money Laundering regulations, and careful consideration of legal frameworks to ensure the legitimacy and security of the cryptocurrency offering.

The research findings underscore the importance of a risk-based approach in Anti-Money Laundering regulations for cryptocurrencies. Recognizing the varying levels of risk associated with different types of cryptocurrencies, regulatory frameworks should be tailored accordingly. This approach allows for more effective allocation of resources, focusing efforts on high-risk areas while minimizing burdens on low-risk activities. The research also emphasizes the need for ongoing monitoring and evaluation of regulatory

frameworks to address emerging risks and adapt to technological advancements in the cryptocurrency industry.

In conclusion, this thesis provides a comprehensive overview of the effective implementation of Anti-Money Laundering regulations in the decentralized and global cryptocurrency industry. It addresses the unique challenges and practical implications of regulating financial crime in this dynamic sector. The research contributes to the existing body of knowledge by offering insights into regulatory clarity, technology-driven solutions, international cooperation, and public-private partnerships. By embracing these recommendations, policymakers and stakeholders can foster a secure and transparent cryptocurrency ecosystem while mitigating the risks of financial crime. The findings of this research pave the way for the development of more effective and coordinated approaches to combat money laundering and illicit activities in the cryptocurrency industry, ensuring its long-term sustainability and integrity.

Table of Contents

Introduction

Cryptocurrencies have emerged as an increasingly popular alternative to traditional forms of currency, with the total market capitalization of all cryptocurrencies exceeding $1.41 trillion as of November 2022.[1] Bitcoin, the first and most well-known cryptocurrency, has been in circulation since 2009[2] and has since been joined by thousands of others, such as Ethereum, Litecoin, and Ripple. The diffusion of cryptocurrencies has been global, with exchanges and wallets available in most countries. Additionally, many merchants, such as online retailers (for example e-commerce websites), that offer goods and services for sale, have begun accepting cryptocurrencies as payment for goods and services, further increasing their popularity.[3]

Despite their growing popularity, cryptocurrencies are also vulnerable to money laundering and other forms of financial crime. The same features that make cryptocurrencies attractive to users, such as a high degree of anonymity and decentralization, can also be exploited by criminals to launder money or fund illegal activities.[4] As such, regulators and law enforcement agencies around the world have been grappling with how to effectively monitor and regulate the use of cryptocurrencies.[5]

Cryptocurrencies have been recognized as potential vehicles for money laundering and other financial crimes, prompting regulators around the world to take steps to implement Anti-Money Laundering (AML) regulations to address these risks.[6] However, implementing AML regulations in the cryptocurrency industry has been a complex and challenging process, due in part to the decentralized and global nature of cryptocurrencies, as well as the lack of clarity around their legal status. Different countries have adopted different approaches to regulation, ranging from outright prohibition to a more laissez-faire approach.[7]

The challenges associated with regulating cryptocurrencies make it an interesting and important area of study. The novelty of cryptocurrencies and the unique challenges they present have made early attempts at regulation particularly important to study. The

---

[1]"Global Cryptocurrency Market Report 2022-2030 | JC Market Research." Yahoo! Finance. Accessed March 10, 2023. https://finance.yahoo.com/news/global-cryptocurrency-market-report-2022-131200732.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABj6LTC6Hen7oZIfOPEfDkIFg4bdokgnGURfMwPehd39PPVQaI3nK46I2NjtiEg6NEcdm23Do_S1OCCr0BTcLqa-Sw1BUQaNOmbAxb9qTi50Tnp85eFt6t088A59qEs6NHpblMGkk1pIFYgNb8fYcyB2ku0UOFZUVz--uE5Lczzz

[2]"Bitcoin Turns 10: An Annotated Timeline." Yahoo! Finance. Accessed March 8, 2023. https://uk.finance.yahoo.com/news/history-bitcoins-first-decade-one-chart-003220581.html

[3]"6 Big Brands That Accept BTC and Why," Binance Blog, accessed March 10, 2023, https://www.binance.com/en/blog/payment/6-big-brands-that-accept-btc-and-why-421499824684903357

[4]Choo, Kim-Kwang Raymond. "Cryptocurrency and Virtual Currency." *Handbook of Digital Currency*, 2015, 283–307. https://doi.org/10.1016/b978-0-12-802117-0.00015-1

[5]*Ibid*

[6]*Ibid*

[7]Omri Marian, "A Conceptual Framework for the Regulation of Cryptocurrencies," University of Chicago Law Review Dialogue 82 (2015-2016): 53-68F

alternatives to regulation are either outright prohibition, which is unlikely to be effective given the decentralized nature of cryptocurrencies, or allowing the cryptocurrency market to operate as a monetary "Wild West", which would likely result in increased risks to consumers and the financial system as a whole.[8]

The legal problem addressed in this research is the implementation of Anti-Money Laundering regulations in the cryptocurrency industry. The main aspects of this problem are the challenges posed by the decentralized and global nature of cryptocurrencies, the lack of clarity surrounding their legal status, and the varying approaches to regulation taken by different countries. This problem is situated within existing legal scholarship that recognizes the potential risks of financial crime associated with cryptocurrencies and the need for effective regulatory measures.

This research paper will explore the implementation of AML regulation in the cryptocurrency industry from an international perspective. It will examine the AML regulations currently in place in different countries, and consider the challenges associated with implementing these regulations in practice and the reasons why other countries impose bans. The paper will also explore potential solutions for addressing these challenges and developing a more effective and coordinated approach to addressing the risks of financial crime in the cryptocurrency industry. In addition, this paper will examine how one particular cryptocurrency, Dukascopy Bank's Dukascoin, is being regulated from an AML perspective in practice. By examining the implementation of AML regulations and particularly the process of creating the own cryptocurrency as an example of a specific cryptocurrency, this paper aims to provide a more detailed and practical understanding of the challenges and opportunities associated with AML regulation in the cryptocurrency industry.

The two main research questions can be highlighted:
How can Anti-Money Laundering regulations be effectively implemented in the decentralized and global cryptocurrency industry, considering its unique characteristics and challenges, in order to mitigate the risks of financial crime?

What are the practical implications and challenges of implementing AML regulations in the cryptocurrency industry, as evidenced by the case of Dukascopy Bank's Dukascoin, and how can these insights contribute to the development of more effective and coordinated approaches to address the risks of financial crime in the sector?

The methodology chosen for this research aims to provide a comprehensive analysis of the implementation of Anti-Money Laundering regulations in the cryptocurrency industry and address the identified research questions effectively. Given the nature of the research problem and the need to gain insights from real-world cases, a mixed-methods approach will be employed.

---

[8]European Central Bank, “For a Few Cryptos More: The Wild West of Crypto Finance,” European Central Bank, April 25, 2022, https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220425~6436006db0.en.html

To address the first research question regarding the effective implementation of AML regulations in the decentralized and global cryptocurrency industry, a qualitative research approach will be utilized. This will involve an in-depth examination of existing AML regulations in different countries, their specific requirements and frameworks, and their practical implications in the cryptocurrency sector. Relevant legal documents, regulatory guidelines, scholarly articles, and case studies will be analyzed to understand the challenges and successes in implementing AML regulations. Additionally, interviews and discussions with regulatory authorities, law enforcement agencies, and industry experts will be examined to gain valuable insights into their perspectives, experiences, and recommendations for effective AML regulation in the cryptocurrency industry. These qualitative data sources will provide a nuanced understanding of the regulatory landscape and help identify best practices and potential areas for improvement.

To address the second research question related to the practical implications and challenges of implementing AML regulations in the cryptocurrency industry, as evidenced by the case of Dukascopy Bank's Dukascoin, a case study methodology will be employed. The Dukascoin case will be analyzed in-depth, considering its specific AML measures, regulatory compliance, and the experiences and outcomes associated with its implementation. This case study will provide practical insights into the challenges faced by a specific cryptocurrency in complying with AML regulations and offer lessons learned for the broader cryptocurrency industry.

The chosen mixed-methods approach combines qualitative research to understand the general regulatory landscape and perspectives, and a focused case study to gain practical insights. This methodology enables a comprehensive examination of the research problem, considering both theoretical and practical dimensions. It allows for the triangulation of data from various sources to enhance the validity and reliability of the findings. The selected methodology aligns with the research questions by providing a detailed exploration of the implementation of AML regulations in the cryptocurrency industry and addressing the specific challenges and practical implications.

The aim of this thesis is to examine the implementation of AML regulations in the cryptocurrency industry and propose strategies for enhancing the AML framework.

To achieve this aim, the following objectives will be pursued:

- Analyze the existing AML regulations in different countries and assess their relevance and effectiveness in the context of the cryptocurrency industry.
- Evaluate the practical implications and challenges associated with the implementation of AML regulations in the cryptocurrency sector.
- Identify best practices and areas for improvement in the AML regulatory framework for cryptocurrencies.
- Develop strategies and recommendations to enhance the effectiveness of AML regulations in the cryptocurrency industry.

- Contribute to existing legal scholarship by providing insights and guidance for policymakers, regulatory authorities, and industry stakeholders.
- Foster a better understanding of the intersection between cryptocurrencies and AML regulations, promoting discussions on innovation, privacy, and the prevention of financial crimes in the digital currency context.

The research has the following limitations:

- Scope and Generalizability: The findings may not apply to specific regional or national contexts with unique regulatory frameworks.
- Evolving Nature: The dynamic cryptocurrency industry may render the research findings less relevant over time.
- Data Limitations: Availability and reliability of data on AML regulations in the cryptocurrency industry may be challenging.
- Legal Complexity: The study may not capture all nuances of specific legal systems or regional regulatory variations.
- Practical Constraints: Conducting empirical research in the sensitive area of AML practices can be challenging due to limited accessibility to information and real-world dynamics.

This thesis consists of three main parts. In the first part, the author explores the terminology and legal aspects related to AML regulation in the field of cryptocurrency. This includes an examination of the AML regulation and terminology in cryptocurrency, the legal framework, and a brief history of EU AML legislation and the Sixth Anti-Money Laundering Directive. The difficulties in regulating cryptocurrency, global cryptocurrency regulation, and existing bans on cryptocurrency are also discussed. The second part focuses on the analysis of the regulation of an existing cryptocurrency, Dukascoin. The author introduces Dukascoin, explains how the Dukascoin currency was put into circulation, and examines the implementation of AML regulation to Dukascoin as a cryptocurrency. The challenges faced by Dukascopy Bank in creating its own cryptocurrency from a legal perspective are also analyzed. The third part analyzes current initiatives and suggests improvements to the existing regulations. The author explores the current initiatives in Switzerland and discusses suggested improvements in the regulations. Additionally, a case law review is conducted, including an analysis of the Tezos case, the Crypto AG case, and other significant cases related to cryptocurrency regulation.

1. Terminology and the legal aspects related to AML regulation in the field of cryptocurrency

1.1 The AML regulation and terminology in cryptocurrency

1.1.1. Terminology

Cryptocurrency is a digital asset that uses cryptography to secure transactions and control the creation of new units. Transactions are recorded on a public ledger, known as a blockchain, which is maintained by a network of computers around the world. A cryptocurrency can be exchanged for goods, services, assets or other currencies.[9]

AML regulations are a set of rules, laws, and procedures designed to prevent money laundering by requiring financial institutions to identify and report suspicious activity.[10] The main goal of AML regulations is to ensure that financial institutions are not being used to facilitate money laundering or other financial crimes.[11] AML regulations require financial institutions to perform due diligence on their customers, monitor transactions for suspicious activity, and report any suspicious activity to the relevant authorities.[12]

In the context of cryptocurrencies, AML regulations serve the same purpose as they do in the traditional financial sector.[13] Cryptocurrencies are considered to be a high-risk area for money laundering and other financial crimes, due in part to the anonymity they provide. [14]AML regulations in the cryptocurrency industry are intended to reduce the risk of financial crime, such as money laundering, terrorist financing, and fraud, by ensuring that cryptocurrency exchanges and other financial institutions are held to the same standards as traditional financial institutions.[15] Additionally, AML regulations can help to promote transparency and increase investor confidence in the cryptocurrency market.[16]

While the primary goal of AML regulations is to prevent financial crime, they can also have other goals, such as protecting national security and ensuring the stability of the financial system.[17] Overall, the implementation of AML regulations in the cryptocurrency

---

[9]The Financial Action Task Force (FATF). 2021. "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF-GAFI, June. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html
[10]Josias N. Dewey, *Global Legal Insights: Blockchain & Cryptocurrency Regulation* (London: Global Legal Group, 2021).
[11]*Ibid*
[12]FATF. "Virtual Currencies: Definitions and Potential AML/CFT Risks." FATF/OECD, June 2014, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
[13]Josias N. Dewey, *supra* note 10.
[14]*Ibid*
[15]Josias N. Dewey, *supra* note 10.
[16]*Supra* note 9
[17]*Ibid*

industry is a complex and challenging process, requiring a careful balance between regulatory oversight and innovation in the rapidly-evolving world of cryptocurrency.[18]

Know Your Customer (KYC) is a process designed to verify the identity of a customer and prevent fraud, money laundering, or terrorist financing.[19] The KYC process typically involves collecting personal information, such as a customer's name, address, and identification documents, and verifying that information using various methods, such as government databases or credit bureaus.[20]

In the context of cryptocurrency, KYC is used to verify the identity of customers who are using a cryptocurrency exchange or other financial institution. However, implementing KYC in the cryptocurrency industry is challenging due to the decentralized and global nature of cryptocurrencies. Cryptocurrency transactions can take place across borders and without intermediaries, making it difficult to establish the identity of the parties involved. Additionally, many cryptocurrency users value their anonymity and may be hesitant to provide personal information to financial institutions.[21]

Despite these challenges, many cryptocurrency exchanges and other financial institutions have implemented KYC procedures in order to comply with AML regulations and reduce the risk of financial crime. Some have even gone beyond regulatory requirements and implemented more stringent KYC procedures to increase the security of their platforms and protect their customers from fraud and hacking attempts. However, the effectiveness of KYC procedures in the cryptocurrency industry is still being evaluated.

Customer Due Diligence (CDD) is the process of assessing the risks associated with a particular customer and monitoring the customer's transactions to identify and report suspicious activity. The CDD process typically involves collecting information about a customer's source of funds, the nature of their business, and their financial history, and then using that information to determine the risk associated with the customer. In the context of cryptocurrency, CDD is used to assess the risk of a customer engaging in financial crime, such as money laundering or terrorist financing.[22]

A Suspicious Activity Report (SAR) is a report that financial institutions must file with regulatory authorities when they suspect that a transaction involves money laundering or other criminal activity. The SAR typically includes details about the suspicious activity, such as the date and time of the transaction, the amount of money involved, and the identity of the

---

[18]*Supra* note 9
[19]Josias N. Dewey, *supra* note 10 p. 12.
[20]*Ibid*
[21]*Supra* note 12 p.12.
[22]Wolfsberg Group. "Wolfsberg's Correspondent Banking Due Diligence Questionnaire (CBDDQ) Glossary." 22 February 2018. Accessed 29 January 2023. https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%27s_CBDDQ_Glossary_220218_v1.0.pdf.

parties involved. In the context of cryptocurrency, SARs are used to report suspicious activity to the relevant authorities.[23]

1.1.2. Legal Framework

The legal framework for AML regulation in the cryptocurrency industry varies by country and is typically designed by the government or a regulatory agency. In the United States, the Financial Crimes Enforcement Network (FinCEN)[24], a bureau of the U.S. Department of the Treasury, is responsible for enforcing AML regulations in the financial sector, including the cryptocurrency industry. Virtual currency exchanges operating in the United States are required to register with FinCEN as money service businesses (MSBs) and comply with the AML regulations established by FinCEN.[25]

FinCEN's AML regulations require MSBs to implement AML programs, including customer identification and transaction monitoring. MSBs must also file Suspicious Activity Reports for suspicious transactions and comply with the record-keeping and reporting requirements of the Bank Secrecy Act (BSA).[26] FinCEN has issued guidance on the application of AML regulations to the cryptocurrency industry, which provides information on how virtual currency businesses can comply with the AML requirements.[27]

In the European Union, the Fifth Anti-Money Laundering Directive (5AMLD)[28] required virtual currency exchanges to register with the relevant national authorities and implement AML programs. The 5AMLD also required virtual currency exchanges to perform Know Your Customer and Customer Due Diligence on their customers, and to file Suspicious Activity Reports when necessary. The 5AMLD also required virtual currency exchanges to maintain records of their transactions for at least five years.[29]

---

[23]"FATF Recommendation 20: Reporting of Suspicious Transactions." Caribbean Financial Action Task Force, www.cfatf-gafic.org/index.php/documents/fatf-40r/386-fatf-recommendation-20-reporting-of-suspicious-transactions.

[24]"United States Department of the Treasury Financial Crimes Enforcement Network," United States Department of the Treasury Financial Crimes Enforcement Network | FinCEN.gov, accessed March 12, 2023, https://www.fincen.gov/

[25]"Law Enforcement Overview," Law Enforcement Overview | FinCEN.gov, accessed March 12, 2023, https://www.fincen.gov/resources/law-enforcement-overview

[26]Szydło, Barbara and Pisarz, Piotr. "Challenges in Regulating Cryptocurrency: A Comparative Analysis of Regulatory Approaches Worldwide." Journal of Risk and Financial Management 13, no. 9 (2020): 203.

[27]Danton Bryans, "Bitcoin and Money Laundering: Mining for an Effective Solution," Indiana Law Journal 89, no. 1 (Winter 2014): 441-472

[28]European Union. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. Official Journal of the European Union, L 156/43, 19 June 2018. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

[29]Szydło, Barbara and Pisarz, Piotr, supra note 26

In 2021, the European Union updated its AML regulation with the Sixth Anti-Money Laundering Directive (6AMLD).[30] The 6AMLD expands the scope of the regulation to cover all virtual currencies, rather than just cryptocurrency exchanges. It also introduces new requirements for enhanced due diligence and greater transparency in beneficial ownership information. The 6AMLD requires EU member states to establish central registers of beneficial ownership information and imposes sanctions for non-compliance with the directive.[31]

In Switzerland, the Financial Market Supervisory Authority (FINMA)[32] is responsible for regulating the cryptocurrency industry and enforcing AML regulations. In 2019, FINMA issued guidelines for virtual asset service providers[33], which includes cryptocurrency exchanges and wallet providers, outlining their obligations under Swiss AML regulations. The guidelines require virtual asset service providers to perform KYC and CDD on their customers, implement transaction monitoring programs, and file SARs when necessary. The guidelines also require virtual asset service providers to maintain records of their transactions for at least five years.[34]

In Asia, countries such as Japan and South Korea have implemented AML regulations for the cryptocurrency industry. In Japan, the Payment Services Act[35] requires virtual currency exchanges to register with the Financial Services Agency (FSA)[36] and to comply with AML regulations. Virtual currency exchanges in Japan are required to implement KYC and CDD procedures and to file SARs when necessary. The FSA also conducts regular inspections of virtual currency exchanges to ensure compliance with AML regulations.[37]

In South Korea, the Act on Reporting and Use of Certain Financial Transaction Information[38] requires virtual currency exchanges to register with the Financial Services Commission (FSC) and to comply with AML regulations. Virtual currency exchanges in South Korea are required to implement KYC and CDD procedures and to file SARs when

---

[30]"Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU" EUR. Accessed May 1, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423

[31]Szydło, Barbara and Pisarz, Piotr, supra note 26 p.14.

[32]Eidgenössische Finanzmarktaufsicht FINMA, "Welcome to the Swiss Financial Market Supervisory Authority Finma," Eidgenössische Finanzmarktaufsicht FINMA, accessed March 12, 2023, https://www.finma.ch/en/

[33]Finma guidance 02/2019 - Eidgenössische Finanzmarktaufsicht Finma. Accessed April 11, 2023. https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20190826-finma-aufsichtsmitteilung-02-2019.pdf?la=en

[34]*Ibid*

[35]Payment services act - english - japanese law translation, accessed March 15, 2023, https://www.japaneselawtranslation.go.jp/en/laws/view/3078/en

[36]Financial Services Agency, accessed March 14, 2023, https://www.fsa.go.jp/en/

[37]Szydło, Barbara and Pisarz, Piotr, supra note 26 p.14.

[38]"Koflu," FIU, accessed April 12, 2023, https://www.kofiu.go.kr/eng/legislation/financial.do#:~:text=The%20Financial%20Transaction%20Reports%20Act%20,%2Fanalysis%2Fdissemination%20of%20STRs

necessary. The FSC also conducts regular inspections of virtual currency exchanges to ensure compliance with AML regulations.[39]

1.1.3. Brief history of EU AML legislation and Sixth Anti-Money Laundering Directive (6AMLD)

The EU has a long history of implementing anti-money laundering directives, with the first directive being adopted in 1991.[40] This directive was primarily focused on combating money laundering in the banking sector and required financial institutions to identify and report suspicious transactions to the relevant authorities. The geopolitical context of this period saw an increase in transnational crime and drug trafficking, leading to greater concerns about money laundering and its potential impact on the financial system.[41]

Since then, the EU has continued to update and strengthen its AML framework in response to evolving threats and new forms of financial innovation. The Second Money Laundering Directive[42] was adopted in 2001, expanding the scope of the first directive to include a wider range of professions and businesses, such as auditors, lawyers, and real estate agents. It also introduced the concept of customer due diligence and enhanced record-keeping requirements. This period saw the aftermath of the 9/11 terrorist attacks, leading to a heightened focus on the financing of terrorism and money laundering as part of global efforts to counter terrorism. [43]

The Third Money Laundering Directive[44] was adopted in 2005, further strengthening the EU's AML framework. It introduced more detailed CDD requirements, including the need to verify customer identity and beneficial ownership. It also introduced the concept of politically exposed persons (PEPs) and required financial institutions to apply enhanced due diligence measures when dealing with PEPs. The adoption of the third directive coincided with increased globalization and cross-border cooperation, which necessitated stronger AML measures to combat money laundering on a global scale.[45]

---

[39] *Ibid*

[40] "Council Directive 91/308/EEC of 10 June 1991 on Prevention of the Use of the Financial System for the Purpose of Money Laundering." EUR. Accessed March 14, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31991L0308

[41] Calin, "History of Anti Money Laundering Directive: A Summary - Part One," ComplyAdvantage, August 25, 2022, https://complyadvantage.com/insights/brief-history-amlds-part-one/

[42] *Ibid*

[43] *Ibid*

[44] "Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance)" EUR, accessed April 12, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0060

[45] Calin, *supra* note 41.

The Fourth Money Laundering Directive[46], adopted in 2015, marked a significant shift towards a risk-based approach to AML. It required financial institutions to carry out risk assessments and implement appropriate measures to mitigate those risks. It also introduced the concept of the beneficial ownership register, which requires companies to disclose information about their ultimate owners.[47] This directive was influenced by the 2012 Financial Action Task Force (FATF) recommendations, which called for a risk-based approach to AML and combating the financing of terrorism.[48]

In addition to the four AMLDs, the EU has also adopted a number of other measures to strengthen its AML framework, including the establishment of the European Banking Authority (EBA) in 2011 and the adoption of the EU's fifth AMLD in 2018. [49]

The need for legislators to keep pace with financial innovation has become increasingly important in recent years, as the rise of new technologies such as cryptocurrency and blockchain have created new challenges for AML efforts. Criminals are increasingly using these technologies to launder money and evade detection, highlighting the need for updated regulations and frameworks that address these new forms of financial innovation.

The Fifth Anti-Money Laundering Directive[50] is a piece of legislation that was introduced by the European Union to strengthen the EU's AML framework. The 5AMLD is aimed at addressing new and emerging money laundering risks, including those associated with virtual currencies, and is applicable to all EU member states.[51] The 5AMLD was a response to the growing use of cryptocurrencies and the increasing need to regulate the virtual currency sector to combat money laundering and terrorist financing risks. [52]

The 5AMLD requires virtual currency exchanges to register with the relevant national authorities and implement AML programs, including customer identification and transaction monitoring. The 5AMLD requires virtual currency exchanges to perform KYC and CDD on their customers, including enhanced due diligence (EDD) for high-risk customers. The 5AMLD also requires virtual currency exchanges to file SARs when necessary.[53]

---

[46]"Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC" EUR. Accessed May 10, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

[47]"EU Context of Anti-Money Laundering and Countering the Financing of Terrorism," Finance, accessed March 16, 2023, https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en#:~:text=The%20European%20Union%20adopted%20the,the%20purpose%20of%20money%20laundering

[48]Calin, "A Brief History of the Amlds: Part Two," ComplyAdvantage, November 24, 2021, https://complyadvantage.com/insights/brief-history-amlds-part-two/

[49]*Supra* note 47, p.16.

[50]*Supra* note 28, p.14.

[51]Zhou, Sarah. "Regulating Cryptocurrencies: Assessing Market Reactions." Journal of Applied Corporate Finance 31, no. 2 (2019): 100-108.

[52]Calin, *supra* note 48.

[53]*Ibid*

One of the most significant changes introduced by the 5AMLD is the requirement for virtual currency exchanges to maintain records of their customers' transactions for at least five years. This requirement is aimed at ensuring that authorities can trace the movement of funds and identify suspicious activity. The 5AMLD also requires member states to establish central registers of beneficial ownership, which will enable authorities to identify the true owners of companies and trusts.[54]

The 5AMLD also introduces new rules for prepaid cards and virtual currency wallet providers. Prepaid card providers are now required to perform KYC and CDD on their customers, and the maximum value of non-reloadable prepaid cards has been reduced from €250 to €150. Virtual currency wallet providers are now subject to the same AML requirements as virtual currency exchanges, including registration with national authorities and the implementation of AML programs.[55]

The 5AMLD also introduces new rules for high-risk third countries. The European Commission is now responsible for identifying high-risk third countries, and virtual currency exchanges are prohibited from carrying out transactions with customers from these countries without conducting additional due diligence. The 5AMLD also requires member states to ensure that their national registers of beneficial ownership are accessible to competent authorities, financial intelligence units, and obliged entities.[56]

The 6th Anti-Money Laundering Directive[57] was introduced in December 2020 and was transposed into national law by EU member states by June 2021. It builds on the previous AMLDs and strengthens the EU's AML framework, particularly in relation to new technologies and the fight against terrorism financing. The directive is a response to the growing threat of terrorism financing and the increasing sophistication of money laundering techniques. It harmonizes the definition of money laundering offenses across EU member states, expands the list of predicate offenses, and introduces stricter sanctions for money laundering offenses.[58]

The 6AMLD includes several key provisions, including the criminalization of certain types of conduct that were previously only subject to administrative sanctions, such as aiding and abetting, inciting, and attempting money laundering. It also introduces new offences, such as the criminalization of money laundering activities committed in relation to a criminal organization and the intentional omission to declare assets located outside the EU.[59]

---

[54]Walker, Clare and Khawar Qureshi. "Implementing the EU's Fifth Anti-Money Laundering Directive: Challenges and Opportunities." Journal of International Banking Law and Regulation (2019): 468-475.
[55]*Supra* note 23 p.13.
[56]*Ibid*
[57]"Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law," EUR, accessed May 1, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.284.01.0022.01.ENG
[58]Calin, *supra* note 48, p.17.
[59]*Supra* note 57.

The 6AMLD also expands the scope of AML obligations to include virtual currency exchanges, custodian wallet providers, and anonymous prepaid card issuers. These entities will be required to carry out customer due diligence measures, report suspicious transactions, and maintain records of transactions for a minimum of five years.[60]

The 6AMLD places an emphasis on enhanced cooperation between EU member states and the use of information-sharing mechanisms to combat money laundering and terrorist financing. To facilitate this cooperation, the directive establishes the European Financial and Economic Crime Centre (EFECC)[61]. The EFECC is a central hub for information-sharing and analysis, founded in June 2020, and is providing support to member states in their efforts to combat financial crime.

The EFECC is tasked with coordinating and facilitating the exchange of information between law enforcement authorities, financial intelligence units, and other relevant bodies across the EU.[62] It will also provide operational and technical assistance to member states, helping to identify emerging threats and trends related to financial crime. The EFECC is expected to play a key role in strengthening the EU's ability to combat money laundering and terrorist financing, and in ensuring effective implementation of the 6AMLD.[63]

In addition to these measures, the 6AMLD introduces more severe sanctions for AML violations, including fines of up to 10% of a company's annual turnover[64], and the possibility of exclusion from public tenders. Member states are also required to ensure that criminal sanctions for AML offences are effective, proportionate, and dissuasive.

Overall, the 6AMLD represents a significant step forward in the EU's efforts to combat money laundering and terrorism financing, particularly in light of the increasing use of new technologies in financial transactions. It emphasizes the importance of cooperation and information-sharing between member states, and imposes stricter obligations and sanctions on entities involved in financial activities. As financial innovation continues to evolve, it is crucial for legislators to keep pace with these developments and ensure that AML legislation remains effective in protecting against financial crime.[65]

---

[60] *Ibid,* p.18.
[61] "European Financial and Economic Crime Centre - EFECC," Europol, accessed March 17, 2023, https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc
[62] *Ibid.*
[63] *Supra* note 61.
[64] Debbie Ward and Bram van Sunder, "How New Rules on Financial Crime Will Impact the EU AML Regime," EY, September 8, 2021, https://www.ey.com/en_gl/financial-services-emeia/how-new-rules-on-financial-crime-will-impact-the-eu-aml-regime
[65] *Ibid.*

1.2 The difficulties in regulating cryptocurrency

1.2.1. Overview of the initial reasons of difficulties in regulation of cryptocurrency

The link between cryptocurrency regulation and the introduction of anti-money laundering legislation targeting cryptocurrencies can be seen in the efforts of governments and financial institutions to combat illicit activities such as money laundering, terrorist financing, and other forms of financial crime. Cryptocurrencies have been seen as a potential tool for criminals to carry out these activities due to their anonymity, lack of central authority, and borderless nature.[66]

A significant challenge in regulating cryptocurrencies is the constant attempt by those being regulated to escape regulation. The decentralized nature of cryptocurrencies makes it difficult for regulators to monitor and enforce compliance, and many cryptocurrency businesses operate outside of traditional financial systems. This has led to a cat-and-mouse game between regulators and cryptocurrency businesses, with regulators struggling to keep up with the rapidly evolving industry.

To address these concerns, governments and financial regulators have introduced AML legislation specifically targeting cryptocurrencies. This legislation requires cryptocurrency exchanges and other service providers to implement measures to detect and prevent money laundering, such as customer due diligence and reporting suspicious transactions to authorities.[67] Some countries have even gone as far as requiring cryptocurrency exchanges to register as money service businesses and obtain AML licenses.

The introduction of AML legislation targeting cryptocurrencies has also had an impact on the development of cryptocurrency regulation more broadly. Many countries have recognized the need for comprehensive cryptocurrency regulation in order to effectively combat financial crime and protect consumers. This has led to the development of regulatory frameworks for cryptocurrencies that incorporate AML measures, such as requiring cryptocurrency businesses to register with financial regulators and comply with AML regulations. [68]

While the introduction of AML legislation targeting cryptocurrencies is a step towards regulating the industry, there are still challenges to overcome. One of the biggest challenges is the global nature of cryptocurrency transactions, which makes it difficult to enforce regulations across borders.

---

[66]Steven Farrugia, Joshua Ellul, and George Azzopardi, "Detection of Illicit Accounts over the Ethereum Blockchain," *Expert Systems with Applications* 150 (2020): 113318, https://doi.org/10.1016/j.eswa.2020.113318
[67]*Supra* note 33, p. 15.
[68]*Ibid*

1.2.2.Anonymity

Anonymity is one of the major challenges in regulating cryptocurrency. Cryptocurrencies are designed to be decentralized, meaning that they are not controlled by any central authority, and transactions are recorded on a public ledger known as the blockchain. While this feature has made cryptocurrencies popular for online transactions, it has also made it difficult for regulatory bodies to regulate them. In this paper, we will delve deeper into the challenges of anonymity in regulating cryptocurrency.[69]

One of the main challenges of anonymity in regulating cryptocurrency is the difficulty in identifying users.[70] Cryptocurrencies are designed to be pseudonymous, meaning that users can transact without providing their real names or personal information. This makes it difficult for regulatory bodies to track down users who may be using cryptocurrencies for illegal activities such as money laundering, terrorism financing, tax evasion, and drug trafficking. While transactions are recorded on the blockchain, the identity of users is not readily available.[71]

Another challenge of anonymity in regulating cryptocurrency is the issue of privacy. Cryptocurrencies were designed to provide users with privacy and anonymity, which is a key selling point for many users.[72] However, this privacy feature has also made it difficult for regulatory bodies to regulate cryptocurrency. Regulating cryptocurrency could infringe on the privacy rights of users, which could lead to backlash from the cryptocurrency community.[73]

Regulatory bodies also face the challenge of limited regulatory powers when it comes to regulating cryptocurrency. Cryptocurrencies are not issued by any central authority, and regulatory bodies do not have the power to control the supply of cryptocurrencies. This means that regulatory bodies cannot regulate the use of cryptocurrencies in the same way that they regulate traditional currencies. This has made it difficult for regulatory bodies to enforce regulations that would prevent the use of cryptocurrencies for illegal activities.[74]

The rise of privacy coins[75] such as Monero[76] and Zcash[77] has made it even more challenging for regulatory bodies to regulate cryptocurrency. Privacy coins are cryptocurrencies that prioritize the privacy and anonymity of their users.[78] They achieve this

---

[69]Virtual currency schemes - a further analysis - European Central Bank, accessed April 13, 2023, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
[70]*Ibid*
[71]FATF. "Guidance on Transparency and Beneficial Ownership." FATF, June 2014, https://www.fatf-gafi.org/content/dam/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.
[72] *Ibid*
[73]*Supra* note 69 p. 20.
[74]*Ibid.*
[75]"What You Need to Know about Privacy Coins," Binance Blog, accessed March 17, 2023, https://www.binance.com/en/blog/fiat/what-you-need-to-know-about-privacy-coins-421499824684903655
[76]GetMonero. "Monero: secure, private, untraceable." Accessed January 28, 2023. https://www.getmonero.org/.
[77]Zcash. Accessed January 28, 2023 https://z.cash/.
[78]Olli-Pekka Hilmola, "On Prices of Privacy Coins and Bitcoin," *Journal of Risk and Financial Management* 14, no. 8 (2021): 361, https://doi.org/10.3390/jrfm14080361

by implementing various measures that conceal the user's identity and transaction details. Some of these measures include ring signatures, stealth addresses, and confidential transactions.[79] Unlike Bitcoin[80], which is pseudonymous and transparent, privacy coins aim to provide users with a high level of anonymity by hiding their transaction details and identities.[81] Bitcoin, is not a privacy coin, as it operates on a public ledger that records all transactions publicly.[82] Ethereum, on the other hand, is not primarily designed as a privacy coin, but it does offer some level of privacy through its smart contracts and decentralized applications (dApps), which can be used to create private transactions and shield user identities.[83]

While users are not required to disclose their real-world identities when transacting with privacy coins like Monero, Zcash, and Ethereum, all transactions are not publicly visible and can be challenging to trace. This anonymity has led some users to seek alternative cryptocurrencies that prioritize privacy and anonymity. However, privacy coins have also been criticized for facilitating illicit activities such as money laundering and terrorist financing, as their anonymity makes it difficult for law enforcement to track these transactions. As a result, some regulatory bodies have proposed or implemented measures to regulate privacy coins or even ban them entirely.[84] This makes it even more difficult for regulatory bodies to track down users who may be using these privacy coins for illegal activities.

1.2.3.Cross-Border Transactions

Cross-border transactions are another significant challenge in regulating cryptocurrency, especially given that cryptocurrencies are global currencies that can be used for transactions across different countries.[85] As such, regulatory bodies face difficulties in regulating cryptocurrency since it is not limited to a specific geographic location. This means that any regulation enacted by one country may not be sufficient to prevent illicit activities that occur in another country.[86]

---

[79]*Ibid,* p.21.
[80]"Open Source P2P Money," Bitcoin, accessed March 14, 2023, https://bitcoin.org/en/
[81]*Supra* note 78.
[82]*Supra* note 80.
[83]"What Is Ethereum?," ethereum.org, accessed March 18, 2023, https://ethereum.org/en/what-is-ethereum/
[84]*Supra* note 78
[85]I Cvetkova, "Cryptocurrencies Legal Regulation," *BRICS Law Journal* 5, no. 2 (2018): 128–53, https://doi.org/10.21684/2412-2343-2018-5-2-128-153
[86]FATF. "Handbook for the Assessment of Vulnerabilities to Money Laundering and Terrorist Financing in the Public Sector - Red Flag Indicators for Virtual Assets." Financial Action Task Force, 2019. Accessed February 8, 2023. https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/Handout-Red-Flags-VA-Public-Sector.pdf.

In the case of online transactions that take place in a virtual space, cross-border transactions refer to transactions that involve parties in different countries.[87] These transactions can occur without any physical presence or interaction between the parties, as they take place entirely in a virtual environment. This virtual nature of cross-border transactions adds another layer of complexity to the challenge of regulating cryptocurrency, as it can be difficult to determine the jurisdiction in which the transaction took place and which regulatory body has the authority to enforce regulations.[88]

One of the main challenges of cross-border transactions in regulating cryptocurrency is jurisdictional issues. Cryptocurrency exchanges can operate from anywhere in the world, and users can transact from any location.[89] This means that regulatory bodies would have to work with other countries to regulate cryptocurrency, which can be a time-consuming and complex process. It also means that regulatory bodies would have to comply with different laws and regulations from different countries.[90]

Another challenge of cross-border transactions in regulating cryptocurrency is the lack of standardization.[91] Cryptocurrencies are not uniform and vary in terms of their functions, security, and usability. This makes it difficult for regulatory bodies to monitor and regulate the different types of cryptocurrencies used for cross-border transactions. It also means that regulatory bodies would have to develop regulations that are specific to each cryptocurrency, which can be a daunting task.[92]

Cross-border transactions in cryptocurrency have made it easier for individuals to launder money. Cryptocurrencies are pseudonymous, which makes it difficult for regulatory bodies to track down individuals who may be using cryptocurrencies to launder money. Criminals can use cryptocurrencies to transfer funds across different countries, making it difficult for law enforcement agencies to track the source and destination of the funds.[93]

Cross-border transactions in cryptocurrency also pose cybersecurity risks. Cryptocurrency exchanges can be targeted by hackers from any location in the world, which can result in significant financial losses for users. This can also make it difficult for regulatory bodies to regulate cryptocurrency as they would have to work with other countries to investigate and prosecute cybercriminals.[94]

---

[87] *Ibid*
[88] *Supra* note 86, p.22.
[89] *Supra* note 85, p.22.
[90] FATF. "Correspondent Banking Services." FATF Recommendations, Financial Action Task Force, 2016, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Correspondent-banking-services.html.
[91] *Supra* note 85, p.22.
[92] Luis Antonio Ahumada, "An Overview of Blockchain and Distributed Ledger Technologies: Architecture, Operation, and Risks," ECB Working Paper No. 2693 (March 2021), accessed February 27, 2023, https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2693~8d4e580438.en.pdf
[93] *Supra* note. 86 p.22.
[94] *Supra* note 90

1.2.4.Lack of Standardization

Lack of standardization is one of the most significant challenges in regulating cryptocurrency. Cryptocurrencies are not uniform and vary in terms of their functions, security, and usability..[95] This lack of standardization makes it challenging for regulatory bodies to regulate cryptocurrency, as they would need to develop regulations specific to each cryptocurrency. Regulators must understand the unique features of each cryptocurrency to develop regulations that address the associated risks..[96] The absence of a standardized framework for cryptocurrency also makes it difficult for businesses and consumers to adopt and use cryptocurrencies. Additionally, the lack of standardization creates challenges for law enforcement agencies when investigating crimes involving cryptocurrencies, as the lack of uniformity makes it challenging to apply existing legal frameworks.[97]

Lack of standardization also poses the risk of regulatory arbitrage. Cryptocurrency exchanges can move to jurisdictions with less stringent regulations to avoid regulatory oversight. This can make it difficult for regulatory bodies to regulate cryptocurrency as they would have to keep up with the ever-changing landscape of cryptocurrency regulation. It can also lead to a race to the bottom as jurisdictions compete to attract cryptocurrency exchanges by offering less stringent regulations.[98]

Lack of standardization also poses a risk to consumer protection. Cryptocurrencies are not backed by any government, and there is no mechanism for consumers to seek recourse in the event of a dispute. This makes it difficult for consumers to protect their investments, which can lead to significant financial losses.[99]

1.2.5.Volatility

Volatility is a significant challenge in regulating cryptocurrency, particularly in the context of anti-money laundering efforts. Cryptocurrencies are known for their high volatility, which makes it difficult for regulatory bodies to regulate and monitor their use effectively. This volatility can be exploited by criminals to launder money, as it allows them to quickly convert funds into cryptocurrency and then back into traditional currency, potentially obscuring the origins of the funds. Additionally, the high volatility of cryptocurrencies can lead to rapid price fluctuations, which can attract criminal activity such as pump-and-dump schemes. The challenge of volatility in the cryptocurrency industry highlights the need for effective AML

---

[95] *Ibid*
[96] International Monetary Fund. "Exploring Multilateral Platforms for Cross-Border Payments." Analytical Notes, January 18, 2023. https://www.imf.org/en/Publications/analytical-notes/Ises/2023/01/18/Exploring-Multilateral-Platforms-for-Cross-Border-Payments-528297.
[97] *Ibid*
[98] Supra note 96
[99] *Ibid*

measures to prevent financial crimes, protect consumers, and maintain the stability of the financial system.[100]

One of the main challenges of volatility in regulating cryptocurrency is the lack of stability. Cryptocurrencies are highly volatile and can experience sudden price fluctuations, making them unpredictable. This makes it difficult for regulatory bodies to develop regulations that are effective in addressing the risks associated with cryptocurrency. [101]

Volatility also poses a risk of market manipulation. Cryptocurrencies are not backed by any government, and their value is determined by supply and demand. This makes them susceptible to market manipulation, as individuals or groups with significant holdings of a cryptocurrency can manipulate the price by buying or selling large amounts of the cryptocurrency. This can lead to significant financial losses for investors and can destabilize the cryptocurrency market.[102]

Another challenge of volatility in regulating cryptocurrency is the difficulty in predicting trends. Cryptocurrencies are highly volatile, and their price can change rapidly based on market conditions. This makes it difficult for regulatory bodies to predict trends and develop effective regulations.[103]

Volatility in cryptocurrency can also impact investment decisions. Investors may be reluctant to invest in cryptocurrency due to its high volatility, which can result in significant financial losses. This can slow down the growth of the cryptocurrency market and make it difficult for regulatory bodies to regulate and monitor its use.[104]

1.2.6.Regulatory Arbitrage

Regulatory arbitrage is another difficulty in regulating cryptocurrency. Cryptocurrency exchanges can choose to operate in jurisdictions that have less stringent regulations. This means that regulatory bodies in countries with stringent regulations may find it difficult to regulate cryptocurrency exchanges that operate in countries with less stringent regulations. This creates a loophole that can be exploited by cryptocurrency exchanges.[105]

Regulatory arbitrage is a significant challenge. It is the practice of moving operations to jurisdictions with less stringent regulations to avoid regulatory oversight. In the context of cryptocurrency, regulatory arbitrage can pose significant challenges for regulators who are trying to develop effective regulations that address the unique risks associated with

---

[100]IMF. "Exploring Multilateral Platforms for Cross-Border Payments." Analytical Notes, January 18, 2023. https://www.imf.org/en/Publications/analytical-notes/Issues/2023/01/18/Exploring-Multilateral-Platforms-for-Cross-Border-Payments-528297.

[101]McGuire, P., and Sushko, V. (2022). "Central bank digital currencies and cross-border payments." Bank for International Settlements Annual Economic Report 2022, chapter 3. Retrieved from https://www.bis.org/publ/arpdf/ar2022e3.htm.

[102]GBBC Council. (2022). The Global Blockchain Business Council: International Journal of Blockchain Law, Volume II. Retrieved from https://gbbcouncil.org/wp-content/uploads/2022/03/IJBL-Volume-II.pdf.

[103]*Supra* note 23 p.13.

[104]*Ibid*

[105]*Supra* note 23 p.13.

cryptocurrency. In this paper, we will delve deeper into the challenges of regulatory arbitrage in regulating cryptocurrency.[106]

One of the main challenges of regulatory arbitrage in regulating cryptocurrency is the difficulty in enforcing regulations. Cryptocurrencies are decentralized, meaning that they are not controlled by any central authority.[107] This makes it difficult for regulatory bodies to enforce regulations as there is no central point of control. Regulators would have to rely on intermediaries such as cryptocurrency exchanges to enforce regulations, which can be challenging as exchanges operate in different jurisdictions.[108]

Regulatory arbitrage can also lead to regulatory competition, where jurisdictions compete to attract cryptocurrency exchanges by offering less stringent regulations. This can make it difficult for regulatory bodies to develop and enforce regulations that are effective in addressing the unique risks associated with cryptocurrency. It can also lead to a race to the bottom as jurisdictions compete to attract cryptocurrency exchanges by offering less stringent regulations.[109]

Regulatory arbitrage can also result in a lack of consistency in regulations across different jurisdictions. This can make it difficult for cryptocurrency exchanges to comply with regulations, as they would have to comply with different regulations in different jurisdictions. It can also lead to confusion among investors who may not be aware of the regulations in different jurisdictions. [110]

Regulatory arbitrage can also pose a risk of money laundering and terrorism financing. Cryptocurrencies are known for their anonymity, which can be exploited by criminals and terrorists to finance illegal activities. If regulatory bodies are unable to enforce regulations effectively due to regulatory arbitrage, it can lead to an increase in money laundering and terrorism financing.[111]

1.3 Global Cryptocurrency regulation

In order to address all these challenges described in previous sub-chapters, a global regulatory framework is required that sets minimum standards for AML/KYC policies and other requirements. Cryptocurrencies, as a relatively new technology, have disrupted traditional financial systems and challenged the way that we think about money.[112] While the technology has many advantages, it also presents unique regulatory challenges that require a

---

[106] *Supra* note 102 p.24.
[107] Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. "Regulatory Arbitrage and the Dark Side of Cryptocurrencies." In The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, edited by David Fox, 393-420. Cambridge University Press, 2019.
[108] *Supra* note 102 p.24.
[109] *Supra* note 107.
[110] *Ibid*
[111] *Ibid*
[112] D. Towne Morton, "The Future of Cryptocurrency: An Unregulated Instrument in an Increasingly Regulated Global Economy," Loyola University Chicago International Law Review 16, no. 1 (Winter 2020): 129-[ii]

global response. One of the most pressing issues is regulatory arbitrage, where different jurisdictions have differing regulatory requirements, creating opportunities for companies to circumvent regulations by moving operations to countries with more lenient rules.[113]

The Basel rules[114], also known as the Basel Accords, refer to a set of international banking regulations that were first introduced in 1988 by the Basel Committee on Banking Supervision (BCBS)[115], serve as an example of a successful global regulatory framework. The rules were established in response to concerns about the stability of the global financial system and the need to prevent another financial crisis like the one that occurred in the early 1980s.[116]

The original Basel rules, also known as Basel I, focused on the minimum capital requirements for banks. These requirements were based on the risk-weighted assets of the bank, with higher-risk assets requiring higher levels of capital. The rules were designed to ensure that banks had sufficient capital to absorb losses and maintain solvency during times of economic stress.[117]

In 2004, the BCBS introduced Basel II, which updated and expanded the original rules. Basel II included new requirements for risk management, including the use of internal risk models by banks to determine their capital requirements. The rules also included new standards for disclosure and transparency, as well as requirements for supervisory review and market discipline.[118]

In response to the global financial crisis of 2008, the BCBS introduced Basel III in 2010. Basel III strengthened the capital requirements for banks and introduced new liquidity requirements to ensure that banks had sufficient cash reserves to meet their obligations during times of stress. Basel III also included new standards for risk management, disclosure, and supervision.[119]

The Basel rules have a significant impact on anti-money laundering regulations in the banking sector. The Basel Committee on Banking Supervision has recognized the importance of AML measures in maintaining the stability of the global financial system.[120] Basel III[121], in particular, includes requirements for banks to have effective AML programs in place, including customer due diligence and transaction monitoring. The rules also require banks to

---

[113] *Ibid*

[114] "History of the Basel Committee," The Bank for International Settlements, October 9, 2014, https://www.bis.org/bcbs/history.htm

[115] "The Basel Committee - Overview," The Bank for International Settlements, June 28, 2011, https://www.bis.org/bcbs/

[116] *Supra* note 114.

[117] *Ibid*

[118] *Supra* note 114

[119] *Ibid*

[120] *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (Washington D.C.: The World Bank, 2006).

[121] Wolters Kluwer, *Banking & Financial Services Policy Report* 30 (May 5, 2011), https://www.weil.com/~/media/files/pdfs/Basel_III_May_2011.pdf

report suspicious transactions to relevant authorities and to comply with AML regulations in all jurisdictions where they operate. The success of the Basel rules in setting global standards for banking regulation provides a potential model for a global regulatory framework for cryptocurrency, including AML measures.[122] A global regulatory framework could establish minimum standards for AML/KYC policies and other requirements, which would help prevent regulatory arbitrage and ensure a consistent approach to cryptocurrency regulation across jurisdictions.[123]

Overall, the Basel rules have been successful in promoting the stability and resilience of the global financial system. However, the implementation of the rules has been uneven, with some countries adopting the rules more quickly and more rigorously than others. This has led to concerns about regulatory arbitrage, where banks can take advantage of differences in regulations between jurisdictions to engage in risky or unethical behavior.

However, implementing such a global regulation is not without challenges. The first challenge is the lack of consensus on what constitutes a cryptocurrency. Different jurisdictions have different definitions of cryptocurrencies, with some countries treating them as currencies while others classify them as assets or securities. This lack of a universal definition makes it difficult to establish a comprehensive regulatory framework that applies to all cryptocurrencies.

The second challenge is the issue of regulatory capture. The cryptocurrency industry has grown rapidly, and it is estimated that the global market capitalization of cryptocurrencies exceeds $1.41 trillion as of November 2022.[124] The industry has significant lobbying power, and it can be difficult for regulators to maintain independence and objectivity when faced with pressure from powerful stakeholders. This challenge highlights the need for transparency in the regulatory process and the importance of avoiding conflicts of interest.[125]

The third challenge is the issue of jurisdiction. Cryptocurrencies operate on a global scale, and it can be difficult to determine which jurisdiction has regulatory authority over them. Furthermore, the lack of consistency in regulations across jurisdictions creates opportunities for regulatory arbitrage, where companies can move operations to countries with more lenient regulations. This challenge highlights the need for a coordinated effort among regulators to establish a global regulatory framework that applies to all jurisdictions.[126]

Despite these challenges, the need for a global regulatory framework for cryptocurrencies is clear. As cryptocurrencies continue to grow in popularity and adoption,

---

[122]Narissa Lyngen, "Basel III: Dynamics of State Implementation," Harvard International Law Journal 53, no. 2 (Summer 2012): 519-536

[123]"Basel Committee Finalises AML/CFT Guidelines on Supervisory Cooperation," The Bank for International Settlements, July 2, 2020, https://www.bis.org/press/p200702.htm

[124]*Supra* note 1 p.8.

[125]Shaen Corbet, *Understanding Cryptocurrency Fraud: The Challenges and Headwinds to Regulate Digital Currencies* (Berlin: De Gruyter, 2022).

[126]*Ibid,* p.27.

the risks associated with them will increase as well. Without proper oversight, the potential for abuse and illicit activities will continue to grow, and the stability and integrity of the financial system will be at risk. A global regulatory framework that sets minimum standards for AML/KYC policies and other requirements will go a long way in mitigating these risks.

1.4 The existing bans on cryptocurrency as an alternative to regulation of cryptocurrency

After discussing the challenges in regulating cryptocurrencies, it is important to also review the bans on digital currencies that have been implemented by some countries. While bans may be seen as a drastic measure, they are often implemented due to concerns about the potential risks associated with cryptocurrencies. These risks include money laundering, terrorist financing, and the destabilizing effect on national currencies and financial systems.

However, it is important to consider whether these bans are effective in addressing these concerns. In many cases, bans may simply drive cryptocurrency-related activities underground, making them even more difficult to regulate and monitor. This can result in an increase in criminal activity and illicit use of digital currencies.

Furthermore, bans can hinder innovation in the blockchain and cryptocurrency space. Cryptocurrencies have the potential to provide many benefits, such as faster and cheaper cross-border transactions and financial inclusion for the unbanked. By banning cryptocurrencies, countries may be missing out on these benefits and stifling the growth of the technology.

Instead of outright bans, countries should consider a more nuanced approach to cryptocurrency regulation that addresses the concerns while allowing for innovation and growth. This may include creating clear regulations and licensing frameworks for cryptocurrency exchanges and service providers, enforcing anti-money laundering and counter-terrorism financing laws, and promoting education and awareness of the risks and benefits of digital currencies.

However, despite the many benefits of cryptocurrency, many countries around the world have banned it. [127] Several countries have implemented bans on cryptocurrency.

1.4.1. China

In 2017, the Chinese government took a series of measures to crack down on cryptocurrency-related activities in the country.[128] One of the key measures was the banning of initial coin offerings (ICOs)[129], which had become a popular way for companies to raise

[127]Hughes, Sarah Jane, and Stephen T. Middlebrook. "Regulating Cryptocurrencies In The United States: Current Issues And Future Directions." Emory Law Journal 68, no. 1 (2018): 195-245.
[128]"China Makes Cryptocurrency Transactions Illegal: An Explainer," China Briefing News, October 21, 2021, https://www.china-briefing.com/news/china-makes-cryptocurrency-transactions-illegal-an-explainer/
[129]"Initial Coin Offerings (ICOS)," SEC Emblem, January 10, 2018, https://www.sec.gov/securities-topics/ICO

funds through cryptocurrency.[130] An ICO is a type of crowdfunding campaign that allows companies to raise money by selling cryptocurrency tokens to investors.[131] The tokens can then be used to access the company's product or service, or they can be traded on cryptocurrency exchanges. However, the Chinese government viewed ICOs as a form of illegal fundraising, as they were not subject to the same regulatory oversight as traditional securities offerings.[132]

As a result, in September 2017, the Chinese government issued a statement declaring ICOs illegal and ordering all fundraising activities to be halted immediately. The statement also called for any funds raised through ICOs to be returned to investors.[133]

In addition to the ICO ban, the Chinese government also cracked down on cryptocurrency mining and trading. Cryptocurrency mining is the process of using powerful computers to solve complex mathematical problems and validate transactions on a blockchain network. In China, cryptocurrency mining had become a major industry, with many companies setting up large-scale mining operations in the country.[134]

However, the Chinese government viewed cryptocurrency mining as a waste of energy and a potential threat to the country's power supply. In response, the government began shutting down cryptocurrency mining operations and even banned cryptocurrency mining in certain provinces.[135]

The Chinese government also took steps to restrict cryptocurrency trading in the country. In early 2018, it issued a ban on all cryptocurrency trading platforms and ordered all cryptocurrency exchanges to shut down. The ban was seen as a way to reduce the risk of fraud and speculation in the cryptocurrency market.[136]

1.4.2. Russia

In July 2019, the Russian government enacted a new law that banned the use of cryptocurrency as a means of payment. The law, which is known as the "Digital Financial

---

[130]John Riley, "The Current Status of Cryptocurrency Regulation in China and Its Effect around the World," *China and WTO Review* 7, no. 1 (2021): 135–52, https://doi.org/10.14330/cwr.2021.7.1.06

[131]Cambridge Centre for Alternative Finance. "Global Cryptoasset Regulatory Landscape Study." Cambridge Judge Business School, University of Cambridge, April 2019. Available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf.

[132]Jia, J., & Wang, W. (2013). Empirical analysis of online forum discussions on Bitcoin. Journal of International Financial Markets, Institutions and Money, 23, 32-44.

[133]*Ibid*

[134]John Riley, *supra* note 130

[135]Xie, Rain. "Why China had to 'Ban' Cryptocurrency but the U.S. did not: A Comparative Analysis of Regulations on Crypto-Markets Between the U.S. and China." Washington University Global Studies Law Review 18, no. 2 (2019).

[136]*Ibid*

Assets" (DFA) law[137], defines cryptocurrency as a type of digital asset that can be traded and owned, but cannot be used to buy goods and services.[138] Under the new law, Russian citizens and companies are prohibited from using cryptocurrency to purchase goods and services, pay bills, or conduct any other financial transactions. Any businesses that violate the law are subject to fines and other penalties.[139]

However, the DFA law does allow for the ownership and trading of cryptocurrency. Russian citizens are still allowed to buy and sell cryptocurrency on exchanges and to hold it as an investment. The law also allows for the use of cryptocurrency in certain types of investment transactions, such as initial coin offerings (ICOs) and other forms of fundraising.[140]

The Russian government's decision to ban the use of cryptocurrency as a means of payment was seen as a move to protect the country's financial system from the risks associated with cryptocurrency, such as money laundering and terrorism financing. The government has also expressed concerns about the volatility of cryptocurrency prices and the potential for fraud and scams in the cryptocurrency market.[141]

1.4.3. Vietnam

In 2018, the government of Vietnam passed a law that banned the use of cryptocurrency as a means of payment. The law, which was titled "On Management and Use of Digital Assets," defined cryptocurrency as a non-lawful means of payment and prohibited individuals and organizations from using it for payments, transactions, or other financial purposes.[142]

In addition to the ban on using cryptocurrency as a means of payment, the law also prohibited financial institutions from offering any cryptocurrency-related services, including issuing, distributing, or providing payment services for cryptocurrency.[143]

The government's decision to ban cryptocurrency was primarily driven by concerns about the potential risks and instability associated with cryptocurrency. The Vietnamese government has stated that it is concerned about the potential for fraud, money laundering, and other illegal activities associated with cryptocurrency. In addition, the government has

---

[137]Russian Government Website, Federal Law of July 31, 2020 No. 259-FZ 'On Digital Financial Assets, Digital Currency, and Amendments to Certain Legislative Acts of the Russian Federation.', Russian Government, July 31, 2020, http://publication.pravo.gov.ru/Document/View/0001202007310056.

[138]*Supra* note 132 p.29.

[139]The Law Library of Congress, Global Legal Research Directorate. "Regulation of Cryptocurrency Around the World: November 2021 Update" (Washington, DC: Library of Congress, 2021)

[140]*Ibid*

[141]"Legislation on circulation of digital financial assets and digital currency to come into force in early 2021." Seamless Legal. Accessed January 31, 2023. https://seamless.legal/en/rus/publication/legislation-on-circulation-of-digital-financial-assets-and-digital-currency-to-come-into-force-in-early-2021.

[142]Dang, Thu Thuy. "Current Situation of Cryptocurrency in Vietnam." Journal of Business, Economics and Environmental Studies 9, no. 4 (2019): 29-34

[143]Thi Ngoc Nga Vu, The Impact of Cryptocurrency on Traditional Financial Markets, April 2022, https://www.theseus.fi/bitstream/handle/10024/753871/Vu_Nga.pdf?sequence=2

expressed concerns about the lack of regulation and oversight in the cryptocurrency market.[144]

Despite the ban on cryptocurrency, there has been some interest in the development of blockchain technology in Vietnam. The government has expressed interest in exploring the use of blockchain in areas such as supply chain management and land registration. However, the use of blockchain technology is currently limited in Vietnam, and there are no specific regulations or guidelines in place for its use.[145]

1.4.4. Bolivia

In 2014, the government of Bolivia issued a decree that effectively banned the use of cryptocurrency in the country.[146] The decree, which was issued by the Bolivian Central Bank, prohibited the use of Bitcoin and other cryptocurrencies for any type of transaction or payment within the country.[147]

The government's decision to ban cryptocurrency was primarily driven by concerns about the lack of regulation and the potential for cryptocurrency to be used in illegal activities, such as money laundering and drug trafficking. The Bolivian government argued that the use of cryptocurrency posed a threat to the country's financial stability and could potentially undermine the ability of the government to regulate the financial system.[148]

Under the decree, any individual or organization that engaged in the use or promotion of cryptocurrency could face criminal charges and penalties. The Bolivian government also warned that it would take action against any businesses or individuals who attempted to circumvent the ban by using cryptocurrency for transactions or payments.[149]

Despite the ban on cryptocurrency, there has been some interest in the development of blockchain technology in Bolivia. In 2018, the Bolivian government announced that it was exploring the use of blockchain technology for voting systems and other government services. However, the use of blockchain technology is currently limited in Bolivia, and there are no specific regulations or guidelines in place for its use.[150]

Overall, the ban on cryptocurrency in Bolivia remains in place, and the government has not shown any signs of reversing its decision.

---

[144] *Ibid,* p. 30.
[145] Clark Sonksen, "Cryptocurrency Regulations in ASEAN, East Asia, & America: To Regulate or Not to Regulate," Washington University Global Studies Law Review 20, no. 1 (2021): 171-200
[146] "Bolivia Essentially Banned Crypto but Blockchain Advocates Are Pushing Back," Yahoo! Finance, accessed April 24, 2023, https://finance.yahoo.com/news/bolivia-essentially-banned-crypto-blockchain-143000382.html
[147] Ghosh, Sharmistha. "Virtual Currency – An Overview." Journal of the Department of Commerce, vol. 4, 2021, pp. 41-50.
[148] Ranvir Singh Sisodia, "Analysis of Cryptocurrency Laws in India and around the World," Law Essentials Journal 2, no. 1 (2021): 233-239
[149] Blockchain Advocates Push Back After Bolivia Essentially Bans Crypto," CoinDesk, December 4, 2020, https://www.coindesk.com/policy/2020/12/04/bolivia-essentially-banned-crypto-but-blockchain-advocates-are-pushing-back/
[150] *Ibid*

1.4.5. Ecuador

The ban on cryptocurrency in Ecuador was enforced through a series of legal and regulatory measures. In February 2014, the National Assembly of Ecuador approved the Organic Monetary and Financial Code, which established the legal framework for the country's financial system and included provisions banning the use of cryptocurrency.[151]

Specifically, Article 94 of the code prohibits the circulation of digital currency, including Bitcoin, within Ecuador.[152] The provision states that "the issuance, production, initiation, circulation, or any other use of digital money is forbidden, as it is not authorized by the competent authority." In addition, Article 95 prohibits the use of digital currency as a means of payment within the country.[153]

The government also issued regulations through the Central Bank of Ecuador to enforce the ban on cryptocurrency. In June 2014, the central bank issued a resolution that declared Bitcoin and other digital currencies to be "not authorized for use in the country's monetary system." The resolution also prohibited financial institutions from transacting in digital currencies or providing services related to digital currency.[154]

Furthermore, in December 2017, the Ecuadorian government passed a law that made it illegal for individuals and businesses to buy, sell, or hold cryptocurrency within the country. The law imposed fines and penalties for violations of the ban on cryptocurrency, and established a regulatory framework for the government's own state-backed digital currency, known as the Electronic Money System.[155]

1.4.6. Reasons for the Bans

Governments around the world have implemented bans on digital currency for a variety of reasons, each of which is reflective of unique political, economic, and social concerns.

One of the most commonly cited reasons for digital currency bans is the lack of regulatory oversight and the potential risks to financial stability. The decentralized nature of digital currencies makes it difficult for governments to monitor transactions and ensure that they adhere to financial regulations. Furthermore, digital currencies are not subject to the same regulatory oversight as traditional financial instruments such as stocks and bonds, which can create a number of risks. For example, the lack of oversight can lead to market

---

[151]"Breaking: Ecuador Bans Bitcoin; Denies Central Bank Issued Digital Currency." CoinDesk, 4 July 2014, https://www.coindesk.com/ecuador-bans-bitcoin-legislative-vote/.
[152]Official Gazette of the Republic of Ecuador, Segundo Suplemento, Año II - Nº 332, Registro Oficial Nº 332, September 12, 2014, https://perma.cc/A69K-7RWU.
[153]*Ibid*
[154]Stan Higgins, "Ecuador Bans Bitcoin, Plans Own Digital Money," CoinDesk Latest Headlines RSS, September 11, 2021, https://www.coindesk.com/markets/2014/07/25/ecuador-bans-bitcoin-plans-own-digital-money/
[155]*Ibid*

manipulation, and digital currencies can be used as a tool for fraud or to engage in illicit activities.[156]

Another key concern for governments is the potential for digital currencies to be used for illegal activities such as money laundering, terrorism financing, and drug trafficking. Digital currencies can provide a high level of anonymity that traditional financial instruments do not, making them particularly attractive to those seeking to evade detection. The use of digital currencies in illicit activities can undermine national security and create risks for law enforcement and regulatory agencies.[157]

In addition to these concerns, some governments view digital currencies as a threat to their own monetary systems. Digital currencies are decentralized, meaning they are not controlled by a single entity such as a government or central bank. This lack of control can create challenges for governments in terms of monetary policy, financial stability, and control over the money supply. Governments may also be concerned that digital currencies could be used to circumvent capital controls and other regulations, potentially destabilizing their own economies.[158]

There are also political reasons for digital currency bans, particularly in countries with authoritarian regimes or unstable political situations. Digital currencies can be used as a means of subverting government control and promoting dissent. In some cases, digital currencies may be viewed as a tool for foreign intervention, as they can be used to circumvent international sanctions and embargoes.[159]

Finally, some governments have implemented digital currency bans simply because they view digital currencies as a threat to their own state-backed currencies. By banning digital currencies, governments can maintain control over their own monetary systems and prevent competition from alternative currencies.[160]

Despite these concerns, some argue that digital currencies offer benefits such as increased financial access and financial inclusion, particularly for those who are unbanked or underbanked. Others argue that digital currencies represent a new era in financial innovation and that governments should embrace them rather than banning them outright.[161]

In response to these debates, some governments have taken a more measured approach to digital currencies, such as Russia's ban on using cryptocurrency as a means of payment while still allowing for ownership and trading. Other countries have implemented regulations aimed at mitigating risks associated with digital currencies, such as the EU's recent proposal for a regulatory framework for crypto assets.[162]

---

[156]Thi Ngoc Nga Vu, *supra* note 143 p.30.
[157]*Supra* note 134 p.29.
[158]Clark Sonksen, *supra* note 145 p.31.
[159]*Ibid.*
[160]*Supra* note 139 p.30.
[161]*Ibid*
[162]*Ibid*

2. The analysis of the regulation of existing cryptocurrency - Dukascoin "DCO"

2.1. What is Dukascoin - "DCO"

2.1.1. Introducing Dukascoin

Dukascoin is a digital asset or cryptocurrency designed and developed by Dukascopy Bank, a Swiss-based financial institution.[163] The primary purpose of Dukascoin is to serve as a secure, efficient, and cost-effective medium of exchange within the bank's digital financial ecosystem. As an innovative financial instrument, Dukascoin is built on the Ethereum blockchain and adheres to the ERC-20 token standard.[164] This ensures its compatibility with a diverse range of digital wallets, decentralized applications, and other blockchain-based services. The emergence of Dukascoin demonstrates the growing interest of traditional financial institutions in the integration of cryptocurrencies and blockchain technology into their business models.[165]

The conception and development of Dukascoin were driven by the increasing demand for secure, transparent, and efficient financial transactions in a globalized economy. The utilization of blockchain technology in the creation of Dukascoin offers numerous advantages over traditional payment systems, such as faster transaction times, lower transaction fees, and a decentralized network infrastructure. By incorporating these advantages into their digital ecosystem, Dukascopy Bank aims to enhance the user experience and streamline various banking processes for its clients.[166]

As a utility token within the Dukascopy ecosystem, Dukascoin allows users to access and participate in an array of services, such as discounted trading fees, premium account services, and staking programs. Moreover, the token can be traded on various digital asset exchanges, providing liquidity and enabling price discovery. The versatile nature of Dukascoin has the potential to attract a broad range of users, from retail clients to institutional investors, thereby fostering increased adoption and utilization of the token.[167]

An essential aspect of Dukascoin's development is its adherence to strict regulatory standards and compliance requirements. By maintaining compliance with regulatory bodies, such as the FINMA, Dukascopy Bank ensures the legitimacy and long-term viability of

---

[163]"Dukascoin. Swiss Bank Cryptocurrency.," RSS, accessed April 4, 2023, https://www.dukascoin.com/
[164]"КОНКУРЕНЦИЯ КРИПТОВАЛЮТ В СОВРЕМЕННОЙ ЭКОНОМИКЕ"(COMPETITION OF CRYPTOCURRENCIES IN THE MODERN ECONOMY), accessed April 17, 2023, https://cyberleninka.ru/article/n/konkurentsiya-kriptovalyut-v-sovremennoy-ekonomike/viewer
[165]*Ibid*
[166]"Dukascoin. Swiss Bank Cryptocurrency.," RSS, accessed April 28, 2023, https://www.dukascoin.com/?cat=wp&page=00
[167]"Volume Trading Commission Discount Program : Dukascopy Bank SA: Swiss Forex Bank: ECN Broker: Managed Accounts: Swiss FX Trading Platform," accessed April 28, 2023, https://www.dukascopy.com/swiss/english/about/fee-schedule/trading-commission-discount-program/

Dukascoin as a digital asset. As a payment token, Dukascoin is subject to specific regulatory frameworks, such as anti-money laundering and know-your-customer policies, which are integral to maintaining the integrity of the token and the broader financial ecosystem.[168]

The emergence of Dukascoin highlights the increasing convergence of traditional financial institutions and digital asset markets. By leveraging the advantages of blockchain technology, Dukascopy Bank has demonstrated the potential of cryptocurrencies to revolutionize the financial sector and promote economic growth. The adoption of Dukascoin, as well as other digital assets, by established financial institutions signifies a shift in the perception and acceptance of cryptocurrencies within the global financial landscape.[169]

Dukascoin represents a novel approach by a traditional financial institution to integrate cryptocurrency and blockchain technology into its operations. Developed by Dukascopy Bank, Dukascoin serves as a medium of exchange, store of value, and unit of account within the bank's digital financial ecosystem. By harnessing the benefits of blockchain technology, such as enhanced security, transparency, and efficiency, Dukascoin has the potential to transform the way financial transactions are conducted and reshape the global financial landscape.

2.1.2. How was the DCO currency put in the circulation

Unlike most cryptocurrencies, which are created through mining, DCO was introduced through a pre-mining process[170] in February 2019. DCO was created through a pre-mining process, in which 3,000,000 DCO were generated by Dukascopy Bank and made available for purchase to its clients. The pre-mining process enabled the bank to establish the initial supply of DCO and allocate tokens to early adopters and investors.

During the pre-mining process, Dukascopy Bank offered DCO at a fixed price of 1 EUR per token, with a minimum purchase amount of 100 DCO. The bank accepted payments in various fiat currencies, including USD, CHF, EUR, GBP, JPY, and CAD. The bank set a cap of 100,000 DCO per client during the pre-mining process to ensure a broad distribution of tokens.[171]

The pre-mining process enabled Dukascopy Bank to raise funds for the development of DCO and its related services, such as the Dukascoin Payment Gateway, which allows merchants to accept DCO as a means of payment.

---

[168]"Dukascoin. Swiss Bank Cryptocurrency.," RSS, accessed April 29, 2023, https://www.dukascoin.com/?lang=en&cat=wp&page=05

[169]*Supra* note 164 p.34.

[170]Adam Hayes, "What Is Premining?," Investopedia, December 30, 2022, https://www.investopedia.com/terms/p/premining.asp

[171]*Supra* note 164 p.34.

After the pre-mining process, Dukascopy Bank launched an initial coin offering to make DCO available to a wider audience. The ICO commenced on 28 March 2019 and was open to both Dukascopy Bank clients and the general public.[172]

The ICO had a soft cap of 10,000,000 DCO and a hard cap of 100,000,000 DCO, with a fixed price of 1 EUR per token. The ICO was conducted in several phases, each with a different bonus structure, to incentivize early participation. The bonus structure ranged from 5% to 50%, depending on the phase of the ICO.[173]

The ICO was conducted through Dukascopy Bank's proprietary platform, Dukascoin Marketplace, which enabled clients to purchase DCO using fiat currencies. The platform required users to complete a KYC procedure, including the provision of Personal Identifiable Information (PII)[174] and documentation, to ensure compliance with AML regulations.

The ICO enabled Dukascopy Bank to raise additional funds for the development of DCO and its related services, such as the Dukascoin Reward Program[175], which rewards users with additional DCO for engaging in trading activities on the bank's internal exchange.

After the ICO, DCO was listed on Dukascopy Bank's internal exchange, Dukascopy Connect 911[176], which enables users to trade DCO and other digital assets. The exchange allows users to trade DCO against fiat currencies, such as USD and EUR, as well as against other cryptocurrencies, such as BTC and ETH.

The trading of DCO on the internal exchange is subject to the bank's rules and regulations, which include strict AML and CTF procedures, transaction monitoring, and reporting of suspicious activities. The bank employs advanced technologies, such as artificial intelligence and machine learning, to ensure the security and transparency of trading activities on its exchange.

The Dukascoin Reward Program, which was launched in May 2019, and incentivizes users to engage in trading activities on the internal exchange by offering additional DCO as a reward, rewards users based on their trading volume and the length of their holding period, with rewards ranging from 5% to 100% of the trading fees paid by users. [177]

The introduction of DCO into circulation involved a pre-mining process, an ICO, and subsequent trading on Dukascopy Bank's internal exchange. The pre-mining process enabled the bank to establish the initial supply of DCO and allocate tokens to early adopters and investors. The ICO allowed the bank to raise additional funds for the development of DCO

---

[172]"Dukascoin. Swiss Bank Cryptocurrency., news" RSS, accessed April 25, 2023, https://www.dukascoin.com/?lang=en&cat=news

[173]*Ibid,* p. 35.

[174]"Guidance on the Protection of Personal Identifiable Information," DOL, accessed April 17, 2023, https://www.dol.gov/general/ppii

[175]"Dukascoin. Swiss Bank Cryptocurrency.," RSS, accessed April 18, 2023, https://www.dukascoin.com/?lang=en&cat=wp&page=06

[176]"Dukascoin. Swiss Bank Cryptocurrency., " RSS, accessed April 17, 2023, https://www.dukascoin.com/?lang=en&cat=wp&page=03

[177]*Supra* note 172 p.35.

and its related services, while the trading on the internal exchange provided liquidity and a trading platform for users.

Throughout the process of introducing DCO into circulation, Dukascopy Bank has adhered to strict AML and CTF regulations to ensure the legitimacy and transparency of the digital asset. The bank's comprehensive AML and CTF framework, encompassing KYC procedures, transaction monitoring, and reporting of suspicious activities, positions DCO as a secure and compliant digital asset in a rapidly evolving regulatory landscape.

2.2 The implementation of AML regulation to the DCO as cryptocurrency and the procedures

The advent of cryptocurrencies and digital assets has presented new challenges for regulatory authorities in combating money laundering and terrorist financing activities. In response to these challenges, regulators have developed anti-money laundering and counter-terrorism financing frameworks to ensure the legitimacy and transparency of digital assets such as Dukascoin.[178]

The regulatory landscape for digital assets and cryptocurrencies is complex and rapidly evolving, with different jurisdictions adopting varying approaches to regulation. In Switzerland, the regulatory framework for digital assets is governed by the FINMA, which oversees financial market activities, including cryptocurrencies and digital assets.[179]

FINMA has classified digital assets into three categories: payment tokens, utility tokens, and asset tokens. Payment tokens, such as Dukascoin, are intended to be used as a means of payment or exchange, while utility tokens are used to access specific services or products. Asset tokens, on the other hand, represent assets such as stocks or bonds.[180]

FINMA requires entities that issue payment tokens to comply with strict AML and CTF regulations, which include KYC procedures, transaction monitoring, and reporting of suspicious activities. These regulations aim to prevent the use of payment tokens for illicit activities, such as money laundering and terrorist financing.[181]

---

[178]CMS Guide to Employment Issues in an M & a transaction, accessed April 11, 2023, https://cms.law/en/media/local/cms-vep/files/publications/guides/cms-guide-to-employment-issues-in-an-m-a-transaction-2014-3?v=1

[179]Eidgenössische Finanzmarktaufsicht FINMA, "Money Laundering: Focus of Conduct Supervision (2021)," Eidgenössische Finanzmarktaufsicht FINMA, accessed April 23, 2023, https://www.finma.ch/en/documentation/dossier/dossier-geldwaeschereibekaempfung/geldwaescherei-schwerpunkte-der-verhaltensaufsicht-2021/

[180]Eidgenössische Finanzmarktaufsicht FINMA, "Developments in Fintech," Eidgenössische Finanzmarktaufsicht FINMA, accessed April 24, 2023, https://www.finma.ch/en/documentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/

[181]Guidelines - Eidgenössische Finanzmarktaufsicht Finma, accessed April 20, 2023, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en

In addition to FINMA, other regulatory bodies such as the Swiss Money Laundering Reporting Office (MROS)[182] and the Swiss Federal Data Protection and Information Commissioner (FDPIC)[183] play a crucial role in ensuring the legality and transparency of digital assets in Switzerland. The MROS is responsible for investigating and prosecuting money laundering and terrorist financing activities, while the FDPIC oversees the protection of personal data related to digital assets and cryptocurrencies.[184] To comply with AML regulations, Dukascopy Bank has developed a comprehensive AML/CTF framework that includes stringent KYC procedures for its clients.

Switzerland has enacted various AML/CTF regulations, which require financial institutions such as Dukascopy Bank to implement specific measures to prevent and detect money laundering and terrorist financing activities. The regulatory provisions applicable to DCO include the Swiss Anti-Money Laundering Act (AMLA)[185], the FINMA Anti-Money Laundering Ordinance (AMLO-FINMA)[186], and FINMA's circular 2016/7 on "Video and Online Identification Procedures."[187]

The Anti-Money Laundering Act in Switzerland requires financial intermediaries, including Dukascopy Bank, to take a risk-based approach to prevent and detect money laundering and terrorist financing activities. This includes implementing internal controls, performing customer due diligence, and reporting suspicious activities to the relevant authorities.

In particular, Article 2 of the AMLA defines financial intermediaries as persons who, professionally or on a commercial basis, accept, hold, manage, invest or transfer assets belonging to others or who assist in the establishment or management of companies.This definition includes banks, securities dealers, and money remitters, among others.[188]

Article 6 of the AMLA requires financial intermediaries to establish and implement an AML program that includes measures to prevent and detect money laundering and terrorist financing activities. This includes performing CDD on customers, which involves identifying and verifying the identity of the customer and beneficial owner, as well as assessing the risk of money laundering and terrorist financing associated with the customer and the transaction.[189]

---

[182]Federal Office of Police, “Money Laundering Reporting Office Switzerland (MROS),” Startseite, accessed April 26, 2023, https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei.html#:~:text=MROS%20is%20a%20member%20of,money%20laundering%20and%20terrorist%20financing..

[183]Task - admin.ch, accessed April 28, 2023, https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/task.html

[184]*Supra* note 178, p.37.

[185]Fedlex, accessed April 29, 2023, https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en

[186]Fedlex, accessed April 30, 2023, https://www.fedlex.admin.ch/eli/cc/2015/390/de

[187]Circular 2016/7 video and online identification - finma.ch, accessed April 26, 2023, https://www.finma.ch/en/~/media/finma/dokumente/rundschreiben-archiv/2016/rs-16-07/finma-rs-2016-07-20180620.pdf?la=en

[188]*Supra* note 185.

[189]*Ibid.*

In addition, Article 9 of the AMLA requires financial intermediaries to report suspicious activities to the Money Laundering Reporting Office Switzerland. This includes any activity that may be related to money laundering or terrorist financing, or that the intermediary has reason to suspect is related to these activities.[190]

In regards to cryptocurrency payments, the Swiss Financial Market Supervisory Authority has issued guidance on the treatment of cryptocurrencies under the AMLA. FINMA considers cryptocurrencies to be assets, and financial intermediaries that accept or hold cryptocurrencies on behalf of customers are subject to the same AML requirements as for traditional assets.[191]

The Anti-Money Laundering Ordinance of the Swiss Financial Market Supervisory Authority specifies the specific measures that financial intermediaries such as Dukascopy Bank must take to comply with the Anti-Money Laundering Act in regards to cryptocurrency payments.[192]

According to Article 10a of the AMLO-FINMA, financial intermediaries must conduct customer due diligence measures, including identification and verification of the identity of the beneficial owner of the assets in case of cryptocurrency payments. This means that Dukascopy Bank must obtain and verify customer identification information, including name, address, and date of birth, and also collect information about the customer's source of wealth and funds.[193]

Furthermore, Article 12 of the AMLO-FINMA specifies the enhanced due diligence measures that must be implemented for high-risk clients, such as PEPs. The bank is required to conduct additional measures to establish the client's identity and assess the risk posed by the relationship. In addition, the bank is required to continuously monitor the business relationship with the client and the transactions conducted within that relationship.[194]

Moreover, Article 9 of the AMLO-FINMA requires financial intermediaries to report any suspicious activities to the relevant authorities, including transactions that appear to be unusual or have no apparent economic or lawful purpose. This includes cryptocurrency transactions that raise suspicion of money laundering or terrorist financing activities.[195]

FINMA's circular 2016/7 applies to financial institutions, including Dukascopy Bank, that use video and online identification procedures to identify their clients remotely, including for cryptocurrency payments.[196] The circular specifies several technical and organizational requirements that must be met, including:

---

[190] *Supra* note 185.
[191] Eidgenössische Finanzmarktaufsicht FINMA, "Finma Guidance: Stringent Approach to Combating Money Laundering on the Blockchain," Eidgenössische Finanzmarktaufsicht FINMA, August 26, 2019, https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/
[192] *Supra* note 186 p.38.
[193] *Ibid*
[194] *Supra* note 186 p.38.
[195] *Ibid*
[196] *Supra* note 187 p.38.

1. Use of secure video technology: Financial institutions must use secure video technology that ensures the confidentiality, integrity, and authenticity of the identification process. The video technology must also allow for real-time interaction between the client and the institution, as well as provide a clear view of the client's face and identification documents.[197]
2. Electronic signatures: Financial institutions must use electronic signatures to document the identification process and the client's consent to the use of remote identification. The electronic signatures must meet the requirements set out in the Swiss Federal Act on Electronic Signatures.[198]
3. Audit trails: Financial institutions must establish and maintain audit trails that record all interactions between the client and the institution during the identification process. The audit trails must be available for inspection by the relevant authorities.[199]

Dukascopy Bank's KYC procedures are designed to comply with these regulations, ensuring that clients are identified, verified, and monitored effectively. The bank collects Personally Identifiable Information and documentation, such as government-issued identification and proof of residence, to verify the identity of its clients. In addition, Dukascopy Bank employs a risk-based approach to identify high-risk clients and transactions, applying EDD measures to gather additional information, such as occupation and employer details, and the source of funds and wealth.

Dukascopy Bank also utilizes transaction monitoring systems to detect and report suspicious activities related to DCO. These systems employ advanced algorithms and artificial intelligence to analyze transaction patterns, identify anomalies, and flag suspicious activities. The transaction monitoring process encompasses several key components, including real-time transaction monitoring, risk-based approach, threshold-based alerts, and reporting of suspicious activities to regulatory authorities.[200] These in more details involve:

1. Real-time transaction monitoring: Dukascopy Bank continuously monitors transactions involving DCO to identify unusual or suspicious patterns. Taking into account quickly changing requirements in this field and sanctions this enables the bank to take immediate action if required. Also, this helps to prevent potential fraudulent transactions which can be tracked during proper transaction monitoring only.[201]
2. Risk-based approach: Dukascopy Bank applies a risk-based approach to transaction monitoring, focusing on high-risk clients, jurisdictions, and transaction types. This allows the bank to allocate resources efficiently and effectively. Risk based approach should be applied not only to real-time transactions but also during monitoring to the client as a whole unit. The things included in analysis include transactional record of a client, his PII information gathered during video identification as much as possibly specific information additionally provided by the client.[202]
3. Threshold-based alerts: The bank sets predefined thresholds for transaction amounts,

---

[197] *Ibid*
[198] *Supra* note 187 p.38.
[199] *Ibid*
[200] *Supra* note 185 p.38.
[201] *Supra* note 187 p.38.
[202] *Ibid*

frequencies, and patterns, triggering alerts if these thresholds are exceeded. This helps identify potential money laundering or terrorist financing activities. This approach is used by various payment institutions to help to divide a big number of transactions on low risk, medium risk and high risk ones, to proceed accordingly and in a timely manner.[203]

4. Reporting: Dukascopy Bank is required to report any suspicious transactions to the appropriate regulatory authorities, such as FINMA or the Swiss Money Laundering Reporting Office. This ensures that potential AML/CTF violations are investigated and addressed.[204]

Also, Dukascopy Bank emphasizes the importance of employee training and awareness in maintaining effective AML/CTF compliance. The bank provides regular training sessions to ensure that employees are familiar with the latest AML regulations, KYC procedures, and transaction monitoring techniques. This ongoing education enables employees to identify and respond to potential AML/CTF risks effectively.[205]

The same important approach applies for record keeping and auditing. Dukascopy Bank maintains comprehensive records of all DCO-related transactions, KYC documentation, and AML/CTF compliance activities. These records are retained for a minimum period, as required by Swiss regulations, typically for ten years.[206] The retention of these records ensures that the bank can provide the necessary information to regulatory authorities during audits or investigations.[207]

Furthermore, Dukascopy Bank undergoes periodic audits by external and internal auditors to assess the effectiveness of its AML/CTF policies and procedures. These audits evaluate the bank's compliance with regulatory requirements, the adequacy of its KYC processes, the effectiveness of its transaction monitoring systems, and the overall implementation of its AML/CTF framework. The findings of these audits inform the bank's continuous improvement efforts and ensure that its AML/CTF policies remain up-to-date and effective.[208]

Also important to note that, in an increasingly interconnected world, international cooperation and information sharing are crucial to combating money laundering and terrorist financing effectively. Dukascopy Bank actively participates in international AML/CTF initiatives and collaborates with other financial institutions, regulatory authorities, and law enforcement agencies to share relevant information and best practices. This cooperation enables the bank to stay informed of emerging AML/CTF risks and adapt its policies and procedures accordingly.[209]

---

[203] *Supra* note 187 p.38.
[204] *Supra* note 187 p.38.
[205] *Supra* note 186 p.38.
[206] Fedlex, accessed April 30, 2023, https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en
[207] *Supra* note 186 p.38.
[208] *Ibid*
[209] *Supra* note 172 p.35.

In addition to AML/CTF regulations, Dukascopy Bank must also comply with international sanctions regimes, such as those imposed by the United Nations, the European Union, and the United States.[210] The bank implements robust sanctions screening processes to ensure that DCO is not used to facilitate transactions involving sanctioned individuals, entities, or countries. This screening involves checking clients and transactions against various sanctions lists and conducting ongoing monitoring to identify potential sanctions violations.[211] As part of their compliance efforts, Dukascopy Bank has taken proactive measures to limit their exposure to sanctioned individuals and entities. For example, the Dukascopy Bank has closed DCO accounts for residents of countries subject to sanctions, such as Russia.[212] The latest eighth package of sanctions adopted by Council tightens the existing prohibitions on crypto-assets by banning all crypto-asset wallets, accounts, or custody services, irrespective of the amount of the wallet (previously up to €10,000 was allowed).[213] By implementing these measures, Dukascopy Bank can ensure that they are not unwittingly facilitating sanctions violations and can continue to operate in compliance with international regulations.

To conclude, the implementation of AML regulations and procedures for DCO demonstrates Dukascopy Bank's commitment to ensuring the legitimacy and transparency of its digital asset. By adhering to stringent AML/CTF requirements, the bank mitigates the risk of DCO being exploited for illicit activities and fosters trust in the token among users, regulators, and the broader financial community. The bank's comprehensive AML/CTF framework, encompassing KYC processes, transaction monitoring, employee training, record keeping, auditing, international cooperation, and sanctions compliance, positions DCO as a secure and compliant digital asset in a rapidly evolving regulatory landscape. The success of DCO and its integration into the global financial ecosystem is contingent upon the effective implementation of AML/CTF measures. As regulatory authorities continue to adapt to the challenges posed by cryptocurrencies and digital assets, Dukascopy Bank must remain vigilant and proactive in maintaining its AML/CTF compliance. By doing so, the bank can ensure the long-term viability and legitimacy of DCO as a digital asset and contribute to the broader effort to combat money laundering and terrorist financing in the cryptocurrency space.

---

[210]Home, accessed May 1, 2023, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Bpp-finsanctions-tf-r6.html

[211]*Supra* note 172 p.35.

[212]"Press Corner," European Commission - European Commission, accessed May 1, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5989

[213]*Ibid*

2.3. Challenges the Dukascopy bank faced in creation of own cryptocurrency from legal perspective

From a legal perspective, the creation of a cryptocurrency by a financial institution such as Dukascopy Bank presents various challenges and considerations. This section examines the specific legal challenges faced by the bank in the creation of DCO, including regulatory compliance, AML and CTF requirements, intellectual property rights, and contractual obligations.

One of the most significant challenges faced by Dukascopy Bank in the creation of DCO was regulatory compliance. The Swiss regulatory framework for cryptocurrencies is complex and rapidly evolving, with various bodies and regulations governing digital assets. To ensure compliance with regulatory requirements, Dukascopy Bank conducted extensive legal research and engaged legal advisors to assess the regulatory landscape and develop a comprehensive legal framework for DCO. This framework includes compliance with AML and CTF regulations, KYC procedures, transaction monitoring, and reporting of suspicious activities.[214]

The bank's legal team also monitored regulatory developments and engaged with regulatory authorities, such as FINMA, to ensure that its legal framework for DCO remained up-to-date and compliant. Taking into account the latest imposition of sanctions, this is a big challenge to keep being up to date and implement all the necessary measures in a timely manner. [215]

As previously discussed, Dukascopy Bank's implementation of AML and CTF requirements for DCO was crucial to ensuring the legitimacy and transparency of the digital asset. However, compliance with these requirements presented legal challenges related to data protection, privacy, and reporting obligations.[216] To address these challenges, the bank's legal team conducted a detailed analysis of data protection and privacy regulations and ensured that its AML and CTF framework for DCO was compliant with these regulations. The bank is using secure servers and internal programs which ensure that the client's personal data is not subject to fraud. The team also developed internal policies and procedures to ensure that reporting obligations were met, while protecting the privacy and confidentiality of client information.[217] This includes measures to prevent phishing and minimize the possibility of human mistake.

The creation of a cryptocurrency also presents challenges related to intellectual property rights, including copyright, trademark, and patent protections. In the case of DCO, the bank had to ensure that its intellectual property rights were protected and that the digital

---

[214] *Supra* note 185 p.38.
[215] *Supra* note 212 p.42.
[216] *Supra* note 185 p.38.
[217] "Switzerland - Data Protection Overview," DataGuidance, December 19, 2022, https://www.dataguidance.com/notes/switzerland-data-protection-overview

asset did not infringe on the intellectual property rights of third parties.[218] To address these challenges, the bank engaged legal advisors to conduct intellectual property searches and assessments to ensure that DCO did not infringe on the intellectual property rights of third parties. The bank also registered DCO as a trademark and filed patent applications for its related services, such as the Dukascoin Payment Gateway.[219]

Moreover, the creation of a cryptocurrency also presents challenges related to contractual obligations, including agreements with clients, suppliers, and service providers. These agreements must ensure compliance with legal requirements, protect the bank's intellectual property rights, and establish clear terms and conditions for the use and trading of DCO. To address these challenges, Dukascopy Bank engaged legal advisors to develop comprehensive agreements with clients, suppliers, and service providers, ensuring compliance with legal requirements and protecting the bank's intellectual property rights. The bank's legal team also reviewed and revised existing agreements to ensure that they were compatible with the legal framework for DCO.

In addition to the challenges mentioned above, the creation of a cryptocurrency also presents other legal considerations that financial institutions must take into account and one such consideration is tax compliance. Cryptocurrencies are still a relatively new asset class, and tax authorities around the world are grappling with how to classify and tax them. In Switzerland, cryptocurrencies are subject to a range of taxes, including income tax, value-added tax (VAT), and wealth tax.[220] To comply with tax requirements, Dukascopy Bank engaged tax advisors to assess the tax implications of DCO and develop a tax strategy for the digital asset.[221]

Another legal consideration for the creation of a cryptocurrency is consumer protection. As cryptocurrencies are a new and relatively unregulated asset class, consumers may be at risk of fraud or loss of funds. Financial institutions must take steps to protect consumers and ensure that they have access to clear and accurate information about the risks and benefits of using and trading cryptocurrencies.[222] To address this consideration, Dukascopy Bank implemented consumer protection measures, such as clear and transparent communication about the risks and benefits of using and trading DCO, and access to customer support and complaint resolution procedures. Company is using secure means of

---

[218]"Trade Mark Protection," Trade mark protection - Swiss Federal Institute of Intellectual Property, accessed May 1, 2023, https://www.ige.ch/en/intellectual-property/all-ip-rights-at-a-glance/trade-mark-protection

[219]White Paper v. 46 09.02.2023 SL on - dukascoin.com, accessed May 2, 2023, https://www.dukascoin.com/media/White-Paper.pdf?v=10546

[220]Administration fédérale des contributions AFC, "Cryptomonnaies – Fiscalité,"(Cryptocurrencies and initial coin/token offerings (ICO/ITO) as subject to wealth, income and profit tax, withholding tax and stamp duty) AFC, accessed May 2, 2023, https://www.estv.admin.ch/estv/fr/accueil/impot-federal-direct/informations-specialisees-ifd/cryptomonnaies.html

[221]*Ibid*

[222]SME Portal, "Swiss and European E-Commerce Laws," Statutory obligations, accessed May 2, 2023, https://www.kmu.admin.ch/kmu/en/home/concrete-know-how/sme-management/e-commerce/creating-own-website/statutory-obligations-in-switzerland-and-the-eu%20.html

communication with the clients and between employees, as well as secure programs for the personal data and other internal data processing.[223]

Furthermore, the creation of a cryptocurrency also raises legal considerations related to cross-border transactions.[224] Cryptocurrencies are a borderless asset, and financial institutions must comply with a range of legal requirements in different jurisdictions when conducting cross-border transactions involving cryptocurrencies.[225] To ensure compliance with cross-border legal requirements, Dukascopy Bank also engaged legal advisors to assess the legal framework for cross-border transactions involving DCO.

In conclusion, the creation of DCO by Dukascopy Bank presented various legal challenges related to regulatory compliance, AML and CTF requirements, intellectual property rights, contractual obligations, tax compliance, consumer protection, and cross-border transactions. The bank addressed these challenges by engaging legal advisors, conducting extensive legal research, and developing a comprehensive legal framework for DCO.

The effective management of legal considerations related to the creation of a cryptocurrency is crucial to ensure the legitimacy and acceptance of the digital asset in the broader financial ecosystem. Dukascopy Bank's approach to addressing legal considerations related to DCO serves as a model for other financial institutions seeking to create and introduce their own digital assets. By adhering to legal requirements and protecting consumer interests, financial institutions can ensure the long-term sustainability and success of their digital assets.

---

[223] *Ibid*

[224] *Ibid*

[225] State Secretariat for International Finance SIF, “Blockchain / DLT,” Staatssekretariat fÃ¼r internationale Finanzfragen SIF - Startseite, accessed May 3, 2023, https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html

3. Analysis of current initiatives and possible improvement of current regulation

3.1 The current initiatives in Switzerland

The Swiss regulatory framework for cryptocurrencies has been instrumental in attracting cryptocurrency startups and fostering innovation in the industry. The principles-based approach to regulation has allowed the country to maintain a flexible and dynamic regulatory environment that allows for innovation and experimentation while ensuring compliance with legal and regulatory requirements.[226]

The licensing requirement for financial institutions that engage in activities related to cryptocurrencies has also contributed to the success of the cryptocurrency industry in Switzerland.[227] The licensing requirement ensures that financial institutions comply with regulatory requirements and maintain the necessary capital adequacy and organizational requirements. The licensing requirement provides greater transparency and accountability, which helps to protect investors and consumers from fraud and other risks associated with cryptocurrencies.[228]

Switzerland's participation in international initiatives to develop a consistent and harmonized regulatory framework for cryptocurrencies further underscores the country's commitment to fostering innovation in the industry while protecting investors and consumers. Switzerland's membership in the GBBC[229] and GDF[230] association is evidence of its leadership in the cryptocurrency industry and its efforts to promote best practices and standards.

The Swiss regulatory framework for cryptocurrencies has been praised for its clarity and consistency. The guidelines issued by FINMA provide clear and transparent communication about the risks and benefits of cryptocurrencies, which is important for investors and consumers. The regulatory landscape for cryptocurrencies is constantly evolving, and Switzerland is taking steps to adapt to new challenges and developments in the industry. The new regulations that were published in 2021 introduce measures to protect investors from fraud and require cryptocurrency issuers and trading platforms to comply with certain requirements. These new regulations ensure that Switzerland maintains its leadership

---

[226]Eidgenössische Finanzmarktaufsicht FINMA, "Principle-Based Regulation," Eidgenössische Finanzmarktaufsicht FINMA, accessed May 3, 2023, https://www.finma.ch/en/finma/activities/regulation/

[227]"Switzerland Crypto License - Crypto License Switzerland, Crypto Exchange License Switzerland, Cryptocurrency License Switzerland." Crypto license, May 9, 2023. https://rue.ee/crypto-licence-in-switzerland/#:~:text=Standard%20initial%20share%20capital%20requirements%20are%20as%20follows%3A&text=98%2C352%20EUR.

[228]*Ibid*

[229]"About GBBC," Global Blockchain Business Council, March 3, 2023, https://gbbcouncil.org/about/

[230]"Global Digital Finance: Advancing Digital Finance," GDF, November 2, 2022, https://www.gdf.io/

position in the cryptocurrency industry while continuing to protect investors and consumers.[231]

Another notable feature of Switzerland's regulatory initiatives for cryptocurrencies is the country's favorable tax environment for cryptocurrency transactions. Switzerland's Federal Tax Administration (FTA)[232] has issued guidelines on the tax treatment of cryptocurrencies, which provide clarity on the tax obligations of individuals and companies that engage in cryptocurrency transactions.

Under Swiss law, cryptocurrencies are treated as assets for tax purposes. Therefore, gains and losses from cryptocurrency transactions are subject to capital gains tax, which is payable on an annual basis. However, the tax rate for capital gains in Switzerland is relatively low compared to other countries, which has helped to attract cryptocurrency businesses and investors to the country.[233]

In addition to the favorable tax environment, Switzerland's regulatory initiatives for cryptocurrencies have also been supported by the country's strong tradition of financial privacy and security.[234] The country's strict data protection laws and regulations provide a high level of security for personal and financial information, which is important for the growth and development of the cryptocurrency industry.[235]

Switzerland's commitment to fostering innovation in the cryptocurrency industry is also reflected in the country's investment in blockchain research and development. Switzerland is home to a number of research centers and initiatives focused on blockchain technology, including the Swiss Blockchain Federation[236] and the Crypto Valley Association.[237]

The Crypto Valley Association is a non-profit organization that supports the development of blockchain and cryptocurrency startups in Switzerland. The association provides networking opportunities, mentoring, and funding to help startups grow and succeed in the industry. The association also works closely with government authorities to ensure that

---

[231] *Supra* note 225 p.44.

[232] Federal Tax Administration FTA, "Federal Tax Administration FTA," EidgenÃ¶ssische Steuerverwaltung - Willkommen, accessed May 4, 2023, https://www.estv.admin.ch/estv/en/home.html#:~:text=rates%20from%202024-,Increase%20in%20VAT%20rates%20from%202024,for%20accommodation%3A%203%2C8%20%25

[233] *Ibid*

[234] Art, money laundering and terrorist financing: New ... - lalive, accessed May 4, 2023, https://www.lalive.law/data/publications/2015-SGI+DLE-Art._money_laundering_and_terrorist_financing_new_developments_in_Swiss_law.pdf

[235] *Ibid*

[236] Für den Erhalt und Ausbau der Attraktivitat und der Konkurrenzfähigkeit des Blockchain-Standorts Schweiz (To maintain and expand the attractiveness and competitiveness of Switzerland as a blockchain location), Blockchain Federation, accessed May 5, 2023, https://blockchainfederation.ch/?lang=en

[237] Crypto Valley Association, accessed May 10, 2023, https://members.cryptovalley.swiss/

the regulatory environment for cryptocurrencies remains favorable for innovation and growth.[238]

Another important regulatory initiative for cryptocurrencies in Switzerland is the country's efforts to develop a legal framework for decentralized finance (DeFi) platforms.[239] DeFi platforms are decentralized applications that allow users to engage in a range of financial activities, such as lending, borrowing, and trading, without the need for intermediaries.[240]

The regulatory framework for DeFi platforms is currently unclear in many jurisdictions, as these platforms are relatively new and operate in a decentralized and often globalized manner. In Switzerland, the legal status of DeFi platforms is still being developed, but there is a clear recognition of the potential benefits of DeFi and the need to ensure regulatory compliance.

In 2020, the Swiss Federal Council published a report on the legal framework for blockchain and distributed ledger technology (DLT), which included a section on DeFi platforms.[241] The report emphasized the need for a principles-based approach to DeFi regulation that balances innovation with investor protection and regulatory compliance. The report also acknowledged the challenges of regulating DeFi platforms, given their decentralized nature and global reach.[242] To address these challenges, the report suggested that DeFi platforms could be subject to the same regulatory requirements as traditional financial institutions, such as AML and CTF compliance, while also recognizing the need for regulatory innovation to address the unique characteristics of DeFi platforms. The report also proposed the development of a sandbox for DeFi platforms, which would allow startups and innovators to experiment with new DeFi applications and business models in a controlled environment.[243] The sandbox would provide regulatory relief and allow for the testing and refinement of new DeFi platforms, while also ensuring that regulatory compliance is maintained.

Another area of current regulatory initiatives for cryptocurrencies in Switzerland is the integration of blockchain technology in the traditional financial system. Switzerland has a long history of innovation in the financial industry, and the country's regulators are actively exploring ways to integrate blockchain technology into traditional financial services. One notable example of this is the use of blockchain technology in the issuance and trading of securities. Switzerland's regulatory framework for securities issuances and trading has been updated to include blockchain-based securities, also known as security tokens. Security

---

[238]"About Us," Crypto Valley Association, accessed May 4, 2023, https://members.cryptovalley.swiss/page/about-us-page

[239] "Decentralized Finance," Decentralized Finance, accessed May 5, 2023, https://www.defi.ch/

[240]*Ibid*

[241]*Supra* note 225 p.44.

[242]*Ibid*

[243]*Supra* note 225 p.44.

tokens are digital assets that represent ownership in a company or asset and can be traded on blockchain-based platforms.[244]

FINMA has issued guidelines for the regulatory treatment of security tokens, which provide clarity on the regulatory requirements for security token issuers and trading platforms. The guidelines require security token issuers to comply with the same regulatory requirements as traditional securities issuers, including AML and CTF compliance and disclosure requirements.[245]

Switzerland's regulatory initiatives for blockchain-based securities have the potential to revolutionize the way securities are issued and traded. Blockchain technology provides greater transparency and efficiency, which can lower costs and increase accessibility to investment opportunities.[246] However, regulatory compliance is essential to ensure investor protection and market stability. In addition to blockchain-based securities, Switzerland is also exploring the use of blockchain technology in other areas of the financial industry, such as payments and settlements. The country's regulators are working with financial institutions and other stakeholders to identify opportunities and challenges in the integration of blockchain technology in the traditional financial system.[247]

Another area of regulatory initiatives for cryptocurrencies in Switzerland is the development of guidelines for stablecoins.[248] Stablecoins are cryptocurrencies that are designed to maintain a stable value relative to a fiat currency, such as the US dollar or Swiss franc. Stablecoins have the potential to address the volatility and price fluctuations that are common in the cryptocurrency market, making them attractive to investors and businesses.[249]

As previously mentioned, the Swiss Federal Council published a report on the legal framework for blockchain and DLT, and it also included a section on stablecoins. The report recognized the potential benefits of stablecoins, such as increased efficiency and lower transaction costs, but also acknowledged the need for regulatory oversight and investor protection.[250] The report recognized the potential benefits of stablecoins, such as increased

---

[244]Eidgenössische Finanzmarktaufsicht FINMA, "Finma Issues First-Ever Approval for a Stock Exchange and a Central Securities Depository for the Trading of Tokens," Eidgenössische Finanzmarktaufsicht FINMA, September 10, 2021, https://www.finma.ch/en/news/2021/09/finma-issues-first-ever-approval-for-a-stock-exchange-and-a-central-securities-depository-for-the-trading-of-tokens/.

[245]*Supra* note 181 p.37.

[246]Galia Kondova and Geremia Simonella, "Blockchain in Startup Financing: Icos and Stos in Switzerland," SSRN, February 27, 2020, https://deliverypdf.ssrn.com/delivery.php?ID=842027003008098069124116094078007110050040086012039063125106092023100102100088123126100002120123037033111096080122013064124080021011055076033018105079105102010125007028082062115121074109010092090114028022090102087075024110078084105096019073081101094092&EXT=pdf&INDEX=TRUE

[247]*Ibid*

[248]State Secretariat for International Finance SIF, "Stablecoins," Staatssekretariat fÃ¼r internationale Finanzfragen SIF - Startseite, accessed May 6, 2023, https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/stablecoins.html

[249]*Ibid*

[250]*Supra* note 225 p.44.

efficiency and lower transaction costs, as well as their potential to facilitate cross-border payments and financial inclusion. However, the report also acknowledged the need for regulatory oversight and investor protection, given the potential risks associated with stablecoins, such as market volatility, liquidity risk, and the risk of fraud or cyberattacks.[251]

The proposed guidelines require stablecoin issuers to obtain a license from FINMA and comply with the same regulatory requirements as traditional financial institutions. Stablecoin issuers are also required to maintain adequate reserves to ensure that the stablecoin remains stable and to protect investors in the event of market fluctuations.[252] Switzerland's approach to stablecoin regulation is similar to its approach to cryptocurrency regulation more broadly, emphasizing the need for regulatory compliance and investor protection while allowing for innovation and experimentation. The proposed guidelines provide clarity and transparency for stablecoin issuers and investors, which is essential for the growth and development of the stablecoin market.

3.2 Suggested improvements in the current regulations

Switzerland's regulatory initiatives for cryptocurrencies are among the most innovative and progressive in the world. However, there is always room for improvement, and stakeholders in the cryptocurrency industry have suggested several areas where the current regulations could be improved to better support the growth and development of the industry. In this chapter, we will explore some of these suggested improvements and their potential impact on the regulatory landscape for cryptocurrencies in Switzerland.[253]

Clarity and consistency in regulatory guidance are critical factors in promoting innovation and investment in the cryptocurrency industry. While the regulatory framework for cryptocurrencies in Switzerland is relatively robust, stakeholders have suggested that the guidelines issued by FINMA lack specificity and clarity in certain areas, which can lead to confusion and uncertainty for businesses and investors. To address this issue, stakeholders have suggested that FINMA provide more specific guidance on certain aspects of cryptocurrency regulation, such as custody and AML compliance. The guidance could be tailored to the specific needs and characteristics of the cryptocurrency industry, providing greater clarity and transparency for businesses and investors.[254]

One area where more specific guidance could be beneficial is custody. Custody is a critical aspect of cryptocurrency investment, as investors need to ensure that their assets are

---

[251] *Supra* note 225 p.44.
[252] *Ibid*
[253] Joanna Diane Caytas, "Regulation of Cryptocurrencies and Initial Coin Offerings in Switzerland: Declared Vision of a 'Crypto Nation,'" *NYSBA International Law Practicum* 31, no. 1 (2018), https://www.blockchainlegalresource.com/wp-content/uploads/sites/31/2018/08/2018IntlPracticumVolume1.pdf#page=53
[254] M. Pravdiuk, "INTERNATIONAL EXPERIENCE OF CRYPTOCURRENCY REGULATION," *Norwegian Journal of Development of the International Science*, 2021, https://doi.org/10.24412/3453-9875-2021-53-2-31-37.

stored securely and are not at risk of theft or fraud. However, the regulatory requirements for custody are not always clear, which can create uncertainty for businesses and investors. To address this issue, FINMA could develop more specific guidance on custody requirements, such as the use of cold storage, multi-signature wallets, and insurance coverage. This would provide greater clarity and transparency for businesses and investors and ensure that regulatory compliance is maintained.[255]

Another area where more specific guidance could be beneficial is AML compliance. AML compliance is critical for the cryptocurrency industry, as it helps to prevent money laundering and other illegal activities. However, the guidelines issued by FINMA on AML compliance are quite broad, which can make it challenging for businesses to know what specific steps they need to take to comply with the regulations. To address this issue, FINMA could develop more specific guidance on AML compliance, such as the specific types of due diligence that businesses should conduct on their customers and the thresholds for reporting suspicious activity. This would provide greater clarity and transparency for businesses and investors and ensure that regulatory compliance is maintained.[256]

In addition to more specific guidance, stakeholders have also suggested that FINMA provide greater consistency in its regulatory guidance. In some cases, the guidelines issued by FINMA are inconsistent with guidelines issued by other regulatory bodies, which can create confusion and uncertainty for businesses and investors. To address this issue, FINMA could work more closely with other regulatory bodies and international organizations to develop a coordinated approach to cryptocurrency regulation. This would ensure that regulatory requirements are consistent and harmonized across different jurisdictions, which would facilitate the development and adoption of cryptocurrencies in the global financial system.[257]

The licensing and regulation of cryptocurrency exchanges is another area where stakeholders have suggested improvement in the current regulatory framework in Switzerland. While the licensing requirement for financial institutions that engage in cryptocurrency activities is a positive development, some stakeholders have argued that the licensing process is too onerous and expensive, particularly for smaller businesses. To address this issue, stakeholders have suggested that FINMA develop a separate licensing regime for cryptocurrency exchanges that is tailored to the specific needs and characteristics of the industry. This would take into account the unique risks associated with cryptocurrency exchanges, such as the risk of theft or fraud, and provide greater flexibility in organizational and capital adequacy requirements.[258]

---

[255]A. Au *et al.*, "Care, Custody, & Control (CCC): Identification, Quantification, and Mitigation of Cryptocurrency Custodial Risk.," *Cryptocurrency and Cyber Risk: Market Analysis and Perspectives*, June 2020.
[256]*Global Legal Insights: Blockchain & Cryptocurrency Regulation* (S.l.: GLOBAL LEGAL GROUP LTD, 2022).
[257]*Supra* note 254 p.50.
[258]*Supra* note 256.

In addition, stakeholders have suggested that FINMA provide more specific guidance on the regulatory requirements for cryptocurrency exchanges, particularly with respect to AML and CTF compliance. This would ensure that exchanges comply with regulatory requirements and maintain the necessary controls to prevent fraud and other risks.[259]

One approach that FINMA could consider is a principles-based approach to regulation. This would allow for greater flexibility and innovation in the industry while ensuring that regulatory compliance is maintained. This could include the development of specific principles and guidelines for exchanges to follow.

Another approach that FINMA could consider is the development of a sandbox for cryptocurrency exchanges. A sandbox would provide a regulatory relief and a controlled environment for startups and innovators to test and refine their business models, while also ensuring that regulatory compliance is maintained. This could encourage greater innovation and investment in the cryptocurrency industry in Switzerland.[260]

Furthermore, Initial Coin Offerings have become a popular way for blockchain startups to raise capital, but they also present significant risks to investors. The current regulatory framework for ICOs in Switzerland is relatively flexible, which has led to a boom in ICO activity in the country. However, stakeholders have suggested that the current regulatory framework could be improved to better protect investors and promote innovation in the industry.[261]

One area where improvements could be made is in the regulatory requirements for ICOs. While FINMA has issued guidelines on ICOs, these guidelines are relatively broad and do not provide specific guidance on the regulatory requirements for ICOs. This can create uncertainty for businesses and investors and may result in regulatory non-compliance. To address this issue, stakeholders have suggested that FINMA provide more specific guidance on the regulatory requirements for ICOs, such as the types of disclosures that must be made to investors and the procedures for conducting due diligence on ICO issuers. This would provide greater clarity and transparency for businesses and investors and ensure that regulatory compliance is maintained.[262]

Another area where improvements could be made is in the flexibility of the regulatory requirements for ICOs. Currently, ICO issuers must comply with the same regulatory requirements as traditional securities offerings, which can be onerous and expensive for startups and small businesses.To address this issue, stakeholders have suggested that FINMA develop a tailored regulatory framework for ICOs that is more flexible and less burdensome

---

[259] *Supra* note 254 p.50.
[260] *Supra* note 255 p.51.
[261] Cristiano Bellavitis, Christian Fisch, and Johan Wiklund, "A Comprehensive Review of the Global Development of Initial Coin Offerings (ICOS) and Their Regulation," *Journal of Business Venturing Insights*, 2021, https://doi.org/10.1016/j.jbvi.2020.e00213
[262] *Ibid*

than the current requirements. This could include exemptions for smaller offerings or simplified disclosure requirements for certain types of offerings.[263]

In addition to these improvements, stakeholders have also suggested that FINMA work more closely with other regulatory bodies and international organizations to develop a coordinated approach to ICO regulation. This would ensure that regulatory requirements are consistent and harmonized across different jurisdictions, which would facilitate the development and adoption of ICOs in the global financial system.[264]

Moreover, taxation is also an important aspect of the regulatory framework for cryptocurrencies in Switzerland. While the tax treatment of cryptocurrencies is relatively straightforward, stakeholders have suggested that the current framework could be improved to provide greater clarity and consistency.[265]

One area where improvements could be made is in the classification of cryptocurrencies for tax purposes. Currently, cryptocurrencies are treated as assets for tax purposes, which means that gains on the sale of cryptocurrencies are subject to capital gains tax. However, stakeholders have suggested that cryptocurrencies should be treated as currency for tax purposes, which would provide greater consistency with other jurisdictions and reduce the tax burden on investors. To address this issue, stakeholders have suggested that FINMA work closely with the Federal Tax Administration to clarify the tax treatment of cryptocurrencies and develop a more consistent and harmonized approach to taxation. This would ensure that investors are not subject to an undue tax burden and would facilitate the growth and adoption of cryptocurrencies in Switzerland.[266]

Another area where improvements could be made is in the tax reporting requirements for cryptocurrency transactions. Currently, there is no requirement for investors to report cryptocurrency transactions on their tax returns, which can create uncertainty and inconsistency in the tax treatment of cryptocurrencies. To address this issue, stakeholders have suggested that FINMA develop more specific guidance on the tax reporting requirements for cryptocurrency transactions. This could include the development of standardized reporting requirements for cryptocurrency transactions or the requirement for investors to report their cryptocurrency holdings on their tax returns.[267]

In addition to these improvements, stakeholders have also suggested that FINMA work closely with other regulatory bodies and international organizations to develop a

---

[263] *Ibid*

[264] *Supra* note 256 p.51.

[265] Ahmet Burçin YERELİ and Işıl Fulya ORKUNOĞLU-ŞAHİN, "Cryptocurrencies and Taxation," *5th International Annual Meeting of Sosyoekonomi Society*, October 25, 2018.

[266] René Zulauf - Partner, Loris Lipp - Manager, and Thomas Ingold - Assistant Manager, "Swiss Tax Authorities Provide Additional Clarity on Crypto-Taxation," Tax and Legal blog, accessed May 7, 2023, https://blogs.deloitte.ch/tax/2022/01/swiss-tax-authorities-provide-additional-clarity-on-crypto-taxation.html

[267] Stephen Turley - Senior Manager and Kristina Bertschinger - Manager, "Cryptocurrencies and Your Swiss Tax Return: Reporting Requirements and Tax Implications," Tax and Legal blog, accessed May 7, 2023, https://blogs.deloitte.ch/tax/2022/04/cryptocurrencies-and-your-swiss-tax-return-reporting-requirements-and-tax-implications.html

coordinated approach to cryptocurrency taxation. This would ensure that the tax treatment of cryptocurrencies is consistent and harmonized across different jurisdictions, which would facilitate the growth and adoption of cryptocurrencies in the global financial system.[268]

However, the integration of blockchain technology into the financial system is also an important development that has the potential to revolutionize the way financial transactions are conducted. While Switzerland has been at the forefront of blockchain innovation, stakeholders have suggested that the current regulatory framework could be improved to better facilitate the integration of blockchain technology into the financial system.[269]

One area where improvements could be made is in the regulatory requirements for blockchain-based financial products and services. Currently, there is a lack of clarity on the regulatory requirements for blockchain-based financial products and services, which can create uncertainty and hinder innovation in the industry. To address this issue, stakeholders have suggested that FINMA provide more specific guidance on the regulatory requirements for blockchain-based financial products and services. This would provide greater clarity and transparency for businesses and investors and ensure that regulatory compliance is maintained.

Another area where improvements could be made is in the development of a supportive regulatory environment for blockchain startups and innovators. While Switzerland has been successful in attracting blockchain startups and innovators, there is a need for greater support from the government and regulatory bodies to ensure that these startups can thrive and innovate. [270]

In addition, stakeholders have also suggested that FINMA work closely with other regulatory bodies and international organizations to develop a coordinated approach to blockchain regulation. This would ensure that regulatory requirements are consistent and harmonized across different jurisdictions, which would facilitate the integration of blockchain technology into the global financial system.

3.3 Case law review

The regulation of cryptocurrencies has been a topic of significant interest and debate in recent years. While some argue that regulation is necessary to protect investors and prevent illicit activities, others view it as potentially stifling innovation and impeding the decentralized nature of cryptocurrencies. To better understand the actual impact and effectiveness of cryptocurrency regulation, it is essential to examine real-world cases and their outcomes. This chapter aims to provide a comprehensive review of selected cases related to cryptocurrency regulation, delving into their specific contexts, regulatory frameworks, and the resulting

---

[268] *Ibid*
[269] *Supra* note 256 p.51.
[270] "Blockchain in Startup Financing: Icos and Stos in Switzerland," *Journal of Strategic Innovation and Sustainability*, February 27, 2020, https://doi.org/10.33423/jsis.v14i6.2607

implications. By analyzing these cases, we can gain valuable insights into the practical implications of cryptocurrency regulation and its effectiveness in achieving its intended goals.

3.3.1.The Tezos case

The Tezos ICO investigation by FINMA was a significant case in the regulation of cryptocurrencies and blockchain technology in Switzerland. Tezos is a blockchain-based platform that allows developers to create smart contracts and decentralized applications. In 2017, Tezos conducted an Initial Coin Offering which raised over $230 million in cryptocurrency, making it one of the largest ICOs at the time.[271]
The ICO was conducted using a complex structure involving the Tezos Foundation, a Swiss-based nonprofit organization, and Dynamic Ledger Solutions (DLS), a Delaware-based corporation founded by the Tezos founders. The ICO offered Tezos tokens (XTZ) to investors in exchange for cryptocurrency such as Bitcoin and Ethereum. Investors were promised that the XTZ tokens would be tradeable on cryptocurrency exchanges once the Tezos platform was launched.[272]

However, the ICO was not without controversy. Shortly after the ICO, several class-action lawsuits were filed against Tezos and its founders, alleging that the ICO constituted an unregistered securities offering in violation of US securities laws. The lawsuits also alleged that Tezos and its founders had made false and misleading statements about the ICO and the Tezos platform.[273]

In Switzerland, FINMA launched an investigation into the Tezos ICO to determine whether the offering violated Swiss financial regulations. The investigation focused on whether the Tezos tokens constituted securities and whether the Tezos Foundation had violated anti-money laundering and counter-terrorist financing regulations.[274]

After an extensive investigation, FINMA ultimately determined that the Tezos ICO did not violate Swiss law. FINMA stated that while the Tezos tokens could be considered securities, they did not meet the criteria for securities under Swiss law. FINMA also found that the Tezos Foundation had complied with Swiss AML and CTF regulations.[275]

However, the investigation highlighted the need for greater regulatory clarity and consistency in the ICO market. FINMA stated that the regulatory requirements for ICOs were

---

[271]Dirk A. Zetzsche et al., "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators," *SSRN Electronic Journal*, 2017, https://doi.org/10.2139/ssrn.3072298
[272]"Tezos ICO Securities Class Action," Restis Law Firm, P.C., August 19, 2021, https://restislaw.com/current-cases-investigations/tezos-initial-coin-offering/
[273]*Supra* note 271.
[274]September 01, Paddy Baker, and CoinDesk, "Tezos Investors Win $25m Settlement in Court Case over $230M ICO," Nasdaq, accessed May 10, 2023, https://www.nasdaq.com/articles/tezos-investors-win-%2425m-settlement-in-court-case-over-%24230m-ico-2020-09-01#:~:text=A%20lawsuit%20alleging%20the%20Tezos,to%20settle%20the%20case%20Friday
[275] *Ibid*

unclear and that there was a lack of consistency in the application of securities laws to ICOs. FINMA recommended that regulatory authorities provide more specific guidance on the regulatory requirements for ICOs and that regulatory requirements be harmonized across different jurisdictions.[276]

The Tezos case also highlights the risks associated with ICOs and the need for greater investor protection. The class-action lawsuits filed against Tezos and its founders demonstrate the potential for investors to suffer significant losses in ICOs, and the need for greater transparency and disclosure in these offerings. The case also underscores the importance of regulatory oversight and enforcement to ensure that ICOs comply with securities laws and regulations. While the Tezos case contributed to increased awareness and accountability within the industry, its long-term impact on shaping cryptocurrency regulation and achieving broader regulatory goals remains a subject of ongoing evaluation.

3.3.2. The Crypto AG case

The Crypto AG scandal was a major case in Switzerland involving the intersection of technology and national security. Crypto AG was a Swiss-based company that provided encryption technology to foreign governments, including the United States and Germany. The company was widely regarded as one of the most secure encryption providers in the world, with its products used by governments, militaries, and intelligence agencies around the globe.[277]

However, in 2018, a joint investigation by The Washington Post and the German public broadcaster ZDF revealed that Crypto AG had been secretly owned and operated by the US Central Intelligence Agency (CIA) and the West German intelligence agency, the BND, since the 1950s. The investigation found that the CIA had inserted a backdoor into Crypto AG's encryption technology, which allowed the agency to access encrypted communications of foreign governments and other targets.[278]

The scandal was significant for several reasons. Firstly, it revealed the extent of US and German intelligence operations and espionage activities during the Cold War and beyond. The revelation that the US and German intelligence agencies had been using Crypto AG's encryption technology to spy on foreign governments and other targets for decades was a major blow to the reputation of both countries.[279]

---

[276] *Supra* note 272.

[277] Vitelio Brustolin, Dennison de Oliveira, and Alcides Eduardo dos Reis Peron, "Exploring the Relationship between Crypto AG and the CIA in the Use of Rigged Encryption Machines for Espionage in Brazil," *Cambridge Review of International Affairs* 36, no. 1 (2020): 54–87, https://doi.org/10.1080/09557571.2020.1842328

[278] *Ibid*

[279] Manuel Rodriguez, "Operation Rubicon: An Assessment with Regard to Switzerland's Duties under the Law of Neutrality," *International Journal of Legal Information* 50, no. 3 (2022): 82–112, https://doi.org/10.1017/jli.2022.31

Secondly, the scandal highlighted the risks associated with the intersection of technology and national security. The fact that a single backdoor in Crypto AG's encryption technology had enabled the CIA and BND to access the communications of countless foreign governments and other targets demonstrated the potential for technology to be exploited for malicious purposes.[280]

Finally, the scandal underscored the need for greater oversight and transparency in the technology industry. The fact that Crypto AG had been secretly owned and operated by the CIA and BND for decades raised questions about the adequacy of existing regulations and oversight mechanisms to prevent such abuses of power.[281]

In Switzerland, the Crypto AG scandal led to calls for greater transparency and accountability in the technology industry. The Swiss government launched an investigation into the matter and announced plans to tighten export controls on surveillance technologies. The scandal also raised questions about the adequacy of existing regulations and oversight mechanisms for encryption technologies and other sensitive technologies.

3.3.3. Other significant cases

Switzerland has been actively engaged in regulating cryptocurrencies and blockchain technology, and as a result, there have been several legal challenges and investigations related to these technologies. One notable case involved FINMA shutting down a fake cryptocurrency company in 2019.

The company, called Quid Pro Quo Association[282], had raised more than $4 million from investors by promising high returns on its cryptocurrency investments. However, FINMA found that the company was not licensed to operate as a financial intermediary in Switzerland and that it had failed to comply with AML and CTF regulations.[283] FINMA launched an investigation into the company and found that it had been conducting unauthorized financial activities and had misled investors about the nature of its business. FINMA also discovered that the company had been using false information to register with various Swiss authorities, including the commercial register and tax authorities.[284] As a result of the investigation, FINMA shut down Quid Pro Quo Association and confiscated its assets. The case demonstrated the importance of regulatory oversight and enforcement in the fight against fraudulent activities in the cryptocurrency industry. It also highlighted the need for

---

[280] *Ibid*
[281] *Ibid*
[282] "Swiss Shut down 'fake' e-Coin in Latest Cryptocurrency Crackdown," Yahoo! Finance, accessed May 11, 2023, https://uk.finance.yahoo.com/news/swiss-shut-down-fake-e-090544871.html
[283] Eidgenössische Finanzmarktaufsicht FINMA, "Finma Closes down Coin Providers and Issues Warning about Fake Cryptocurrencies," Eidgenössische Finanzmarktaufsicht FINMA, September 19, 2017, https://www.finma.ch/en/news/2017/09/20170919-mm-coin-anbieter/
[284] *Supra* note 271, 55.

greater vigilance and due diligence by investors in assessing the legitimacy of cryptocurrency offerings.[285]

Another significant case in Switzerland involved the cryptocurrency exchange, E-Coin, which was forced to shut down its operations in 2016 after the FINMA determined that the exchange had violated Swiss banking regulations. FINMA found that E-Coin had been operating without a license and had failed to comply with AML and CTF regulations.[286]

The case highlighted the importance of licensing and regulation for cryptocurrency exchanges, as well as the need for compliance with AML and CTF regulations to prevent money laundering and terrorist financing activities.

Another case involved the Swiss blockchain company, Envion AG, which raised over $100 million in an ICO in 2018. The company was later involved in a legal dispute between its founders and shareholders, which resulted in a court order to liquidate the company. The case highlighted the risks associated with ICOs and the need for greater transparency and disclosure in these offerings.[287]

In addition to these cases, there have been several other legal challenges and investigations related to cryptocurrencies and blockchain technology in Switzerland. These cases have demonstrated the importance of regulatory oversight and enforcement to protect investors and ensure the integrity of the market. They have also highlighted the need for greater clarity and consistency in the regulatory landscape, as well as the importance of compliance with AML and CTF regulations to prevent fraudulent activities and protect against money laundering and terrorist financing activities.

---

[285] *Supra* note 283.

[286] *Ibid*

[287] Eidgenössische Finanzmarktaufsicht FINMA, "Finma Ascertains Illegal Activity by Envion AG," Eidgenössische Finanzmarktaufsicht FINMA, March 27, 2019, https://www.finma.ch/en/news/2019/03/20190327---mm---envion/

Conclusion

In conclusion, this thesis has provided a comprehensive examination of the implementation of Anti-Money Laundering (AML) regulations in the decentralized and global cryptocurrency industry. The research has addressed the research questions regarding how AML regulations can be effectively implemented considering the unique characteristics and challenges of the industry, and the practical implications and challenges of implementing AML regulations in the case of Dukascopy Bank's Dukascoin (DCO). Through this analysis, several key findings and contributions have emerged.

Firstly, effective implementation of AML regulations in the cryptocurrency industry requires a multifaceted approach that takes into account the industry's unique characteristics and challenges. The decentralized nature of cryptocurrencies, coupled with the global reach and high degree of anonymity, necessitates regulatory frameworks that are adaptable, technology-neutral, and globally coordinated. The research has highlighted the importance of striking a balance between regulatory compliance and fostering innovation, recognizing that overly burdensome regulations can stifle industry growth and technological advancements.

The analysis of the Dukascoin case has provided valuable insights into the practical implications and challenges of implementing AML regulations in a specific cryptocurrency project. The case highlighted the significance of thorough legal assessments and compliance with regulatory requirements, demonstrating the importance of regulatory oversight and enforcement mechanisms to ensure the integrity and stability of cryptocurrencies. The findings from the Dukascoin case serve as a valuable reference for policymakers, regulators, and industry participants in understanding the complexities and practical considerations associated with implementing AML regulations in the cryptocurrency sector.

Furthermore, this research has shed light on the need for regulatory clarity and consistency across jurisdictions. The lack of harmonization in AML regulations for cryptocurrencies poses challenges for industry participants, as they navigate a complex web of varying regulatory requirements. The analysis has emphasized the importance of collaboration and coordination among regulatory bodies and international organizations to establish common standards and share best practices. This collaborative approach will contribute to the development of a more effective and globally coordinated regulatory framework that can address the risks of financial crime in the cryptocurrency industry.

Moreover, this thesis has highlighted the significance of investor protection in the implementation of AML regulations. The cryptocurrency industry has witnessed fraudulent activities and scams that have resulted in financial losses for investors. The research has underscored the importance of transparency, disclosure, and due diligence in cryptocurrency offerings to safeguard investor interests. Regulatory frameworks should aim to provide clear guidelines and requirements for cryptocurrency projects, ensuring that investors have access to accurate and reliable information to make informed investment decisions.

The research has also identified the challenges associated with implementing AML regulations in the cryptocurrency industry. The decentralized and pseudonymous nature of cryptocurrencies poses ongoing challenges for effective regulatory oversight. The rapid pace of technological advancements, cross-border transactions, and evolving methods of financial crime necessitate continuous monitoring and adaptation of regulatory approaches. Policymakers and regulators must stay abreast of industry developments, engage in ongoing dialogue with industry stakeholders, and leverage technology-driven solutions, such as blockchain analytics, to enhance the effectiveness of AML regulations.

This thesis has contributed to the understanding of the implementation of AML regulations in the decentralized and global cryptocurrency industry. The analysis has provided valuable insights into the challenges and opportunities of implementing AML regulations, particularly through the examination of the Dukascoin case. The findings emphasize the need for regulatory frameworks that are adaptable, globally coordinated, and investor-focused, while also fostering innovation and technological advancements. The research underscores the importance of regulatory clarity, consistency, and collaboration among international stakeholders to address the risks of financial crime in the evolving cryptocurrency industry. By adopting a comprehensive and balanced approach, regulators can mitigate the risks associated with money laundering and other financial crimes, while supporting the growth and development of the cryptocurrency ecosystem.

In addition to the specific findings and contributions outlined above, this thesis has broader implications for the development of more effective and coordinated approaches to address the risks of financial crime in the cryptocurrency industry. By examining the challenges, practical implications, and lessons learned from the implementation of AML regulations, policymakers, regulators, and industry participants can gain valuable insights to shape future regulatory frameworks and practices.

One of the key contributions of this research is the emphasis on the importance of technology-driven solutions in enhancing AML regulations in the cryptocurrency industry. Blockchain analytics and other innovative tools have the potential to enhance the detection and prevention of money laundering and illicit activities. By leveraging these technologies, regulators can gain greater visibility into cryptocurrency transactions and identify suspicious patterns more efficiently. The integration of these solutions into regulatory frameworks can improve the effectiveness of AML regulations and enhance the overall security of the cryptocurrency ecosystem.

Furthermore, the research has highlighted the need for continuous monitoring and adaptation of AML regulations in response to evolving risks and challenges. The cryptocurrency industry is dynamic, with new technologies, business models, and risks emerging regularly. It is crucial for regulators to remain proactive and flexible, regularly reviewing and updating regulatory frameworks to address emerging risks effectively. Close collaboration with industry stakeholders, technology experts, and international partners is

essential to stay ahead of evolving trends and ensure the ongoing effectiveness of AML regulations.

Another significant contribution of this thesis is the identification of the importance of international cooperation and harmonization in combating financial crime in the cryptocurrency industry. Given the global nature of cryptocurrencies and the potential for cross-border transactions, a fragmented and inconsistent regulatory landscape can undermine the effectiveness of AML efforts. This research highlights the need for increased cooperation among regulators, international organizations, and industry associations to establish common standards, share information, and develop coordinated strategies. Through such collaboration, the global fight against financial crime can be strengthened, and regulatory arbitrage can be minimized.

Additionally, the research emphasizes the significance of public-private partnerships in addressing the risks of financial crime in the cryptocurrency industry. Governments and regulators should work closely with cryptocurrency businesses, exchanges, and other industry stakeholders to establish robust compliance frameworks, enhance transparency, and promote responsible business practices. Collaboration between the public and private sectors can foster innovation, create a level playing field, and ensure that AML regulations are both effective and feasible for industry participants.

In conclusion, this thesis has provided a comprehensive analysis of the implementation of AML regulations in the decentralized and global cryptocurrency industry. Through the examination of the challenges, practical implications, and case study of Dukascoin, valuable insights have been gained into the complex nature of regulating financial crime in this evolving sector. The findings highlight the need for adaptable, globally coordinated, and technology-driven regulatory frameworks that prioritize investor protection while fostering innovation. The research underscores the importance of regulatory clarity, consistency, continuous monitoring, international cooperation, and public-private partnerships in effectively addressing the risks of financial crime in the cryptocurrency industry. By applying these insights and recommendations, policymakers, regulators, and industry participants can contribute to the development of more effective and coordinated approaches to mitigate the risks of financial crime and foster the growth of a secure and trustworthy cryptocurrency ecosystem.

Bibliography

1. “Decentralized Finance,” Decentralized Finance, accessed May 5, 2023, https://www.defi.ch/
2. Joanna Diane Caytas, “Regulation of Cryptocurrencies and Initial Coin Offerings in Switzerland: Declared Vision of a ‘Crypto Nation,’” NYSBA International Law Practicum 31, no. 1 (2018), https://www.blockchainlegalresource.com/wp-content/uploads/sites/31/2018/08/2018IntlPracticumVolume1.pdf#page=53
3. "Breaking: Ecuador Bans Bitcoin; Denies Central Bank Issued Digital Currency." CoinDesk, 4 July 2014, https://www.coindesk.com/ecuador-bans-bitcoin-legislative-vote/.
4. "FATF Recommendation 20: Reporting of Suspicious Transactions." Caribbean Financial Action Task Force, www.cfatf-gafic.org/index.php/documents/fatf-40r/386-fatf-recommendation-20-reporting-of-suspicious-transactions.
5. "Legislation on circulation of digital financial assets and digital currency to come into force in early 2021." Seamless Legal. Accessed January 31, 2023. https://seamless.legal/en/rus/publication/legislation-on-circulation-of-digital-financial-assets-and-digital-currency-to-come-into-force-in-early-2021.
6. “‘КОНКУРЕНЦИЯ КРИПТОВАЛЮТ В СОВРЕМЕННОЙ ЭКОНОМИКЕ’’(COMPETITION OF CRYPTOCURRENCIES IN THE MODERN ECONOMY), accessed April 17, 2023, https://cyberleninka.ru/article/n/konkurentsiya-kriptovalyut-v-sovremennoy-ekonomike/viewer
7. “6 Big Brands That Accept BTC and Why,” Binance Blog, accessed March 10, 2023, https://www.binance.com/en/blog/payment/6-big-brands-that-accept-btc-and-why-421499824684903357
8. “About GBBC,” Global Blockchain Business Council, March 3, 2023, https://gbbcouncil.org/about/
9. “About Us,” Crypto Valley Association, accessed May 4, 2023, https://members.cryptovalley.swiss/page/about-us-page
10. “Basel Committee Finalises AML/CFT Guidelines on Supervisory Cooperation,” The Bank for International Settlements, July 2, 2020, https://www.bis.org/press/p200702.htm
11. “Bitcoin Turns 10: An Annotated Timeline.” Yahoo! Finance. Accessed March 8, 2023. https://uk.finance.yahoo.com/news/history-bitcoins-first-decade-one-chart-003220581.html.
12. “Blockchain in Startup Financing: Icos and Stos in Switzerland,” Journal of Strategic Innovation and Sustainability, February 27, 2020, https://doi.org/10.33423/jsis.v14i6.2607
13. “Bolivia Essentially Banned Crypto but Blockchain Advocates Are Pushing Back,” Yahoo! Finance, accessed April 24, 2023,

https://finance.yahoo.com/news/bolivia-essentially-banned-crypto-blockchain-143000382.html
14. “China Makes Cryptocurrency Transactions Illegal: An Explainer,” China Briefing News, October 21, 2021, https://www.china-briefing.com/news/china-makes-cryptocurrency-transactions-illegal-an-explainer/
15. “Council Directive 91/308/EEC of 10 June 1991 on Prevention of the Use of the Financial System for the Purpose of Money Laundering.” EUR. Accessed March 14, 2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31991L0308
16. “Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC” EUR. Accessed May 10, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849
17. “Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law,” EUR, accessed May 1, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.284.01.0022.01.ENG
18. “Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU” EUR. Accessed May 1, 2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423
19. “Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance)” EUR, accessed April 12, 2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0060
20. “Dukascoin. Swiss Bank Cryptocurrency., ” RSS, accessed April 17, 2023, https://www.dukascoin.com/?lang=en&cat=wp&page=03
21. “Dukascoin. Swiss Bank Cryptocurrency., news” RSS, accessed April 25, 2023, https://www.dukascoin.com/?lang=en&cat=news
22. “Dukascoin. Swiss Bank Cryptocurrency.,” RSS, accessed April 18, 2023, https://www.dukascoin.com/?lang=en&cat=wp&page=06
23. “Dukascoin. Swiss Bank Cryptocurrency.,” RSS, accessed April 28, 2023, https://www.dukascoin.com/?cat=wp&page=00
24. “Dukascoin. Swiss Bank Cryptocurrency.,” RSS, accessed April 29, 2023, https://www.dukascoin.com/?lang=en&cat=wp&page=05.
25. “Dukascoin. Swiss Bank Cryptocurrency.,” RSS, accessed April 4, 2023, https://www.dukascoin.com/
26. “EU Context of Anti-Money Laundering and Countering the Financing of Terrorism,” Finance, accessed March 16, 2023,

https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en#:~:text=The%20European%20Union%20adopted%20the,the%20purpose%20of%20money%20laundering
27. “European Financial and Economic Crime Centre - EFECC,” Europol, accessed March 17, 2023, https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc
28. “European Union. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU”. Official Journal of the European Union, L 156/43, 19 June 2018. Accessed May 1, 2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843
29. “Global Cryptocurrency Market Report 2022-2030 | JC Market Research.” Yahoo! Finance. Accessed March 10, 2023. https://finance.yahoo.com/news/global-cryptocurrency-market-report-2022-131200732.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABj6LTC6Hen7oZIfOPEfDkIFg4bdokgnGURfMwPehd39PPVQaI3nK46I2NjtiEg6NEcdm23Do_S1OCCr0BTcLqa-Sw1BUQaNOmbAxb9qTi50Tnp85eFt6t088A59qEs6NHpblMGkk1pIFYgNb8fYcyB2ku0UOFZUVz--uE5Lczzz
30. “Global Digital Finance: Advancing Digital Finance,” GDF, November 2, 2022, https://www.gdf.io/
31. “Guidance on the Protection of Personal Identifiable Information,” DOL, accessed April 17, 2023, https://www.dol.gov/general/ppii
32. “History of the Basel Committee,” The Bank for International Settlements, October 9, 2014, https://www.bis.org/bcbs/history.htm
33. “Initial Coin Offerings (ICOS),” SEC Emblem, January 10, 2018, https://www.sec.gov/securities-topics/ICO
34. “Koflu,” FIU, accessed April 12, 2023. Available at: https://www.kofiu.go.kr/eng/legislation/financial.do#:~:text=The%20Financial%20Transaction%20Reports%20Act%20,%2Fanalysis%2Fdissemination%20of%20STRs
35. “Law Enforcement Overview,” Law Enforcement Overview | FinCEN.gov, accessed March 12, 2023, https://www.fincen.gov/resources/law-enforcement-overview
36. “Open Source P2P Money,” Bitcoin, accessed March 14, 2023, https://bitcoin.org/en/
37. “Press Corner,” European Commission - European Commission, accessed May 1, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5989
38. “Swiss Shut down ‘fake’ e-Coin in Latest Cryptocurrency Crackdown,” Yahoo! Finance, accessed May 11, 2023, https://uk.finance.yahoo.com/news/swiss-shut-down-fake-e-090544871.html
39. “Switzerland - Data Protection Overview,” DataGuidance, December 19, 2022, https://www.dataguidance.com/notes/switzerland-data-protection-overview
40. “Switzerland Crypto License - Crypto License Switzerland, Crypto Exchange License Switzerland, Cryptocurrency License Switzerland.” Crypto license, May 9, 2023. https://rue.ee/crypto-licence-in-switzerland/#:~:text=Standard%20initial%20share%20capital%20requirements%20are%20as%20follows%3A&text=98%2C352%20EUR.

41. “Tezos ICO Securities Class Action,” Restis Law Firm, P.C., August 19, 2021, https://restislaw.com/current-cases-investigations/tezos-initial-coin-offering/
42. “The Basel Committee - Overview,” The Bank for International Settlements, June 28, 2011, https://www.bis.org/bcbs/
43. “Trade Mark Protection,” Trade mark protection - Swiss Federal Institute of Intellectual Property, accessed May 1, 2023, https://www.ige.ch/en/intellectual-property/all-ip-rights-at-a-glance/trade-mark-protection
44. “United States Department of the Treasury Financial Crimes Enforcement Network,” United States Department of the Treasury Financial Crimes Enforcement Network | FinCEN.gov, accessed March 12, 2023, https://www.fincen.gov/
45. “Volume Trading Commission Discount Program : Dukascopy Bank SA: Swiss Forex Bank: ECN Broker: Managed Accounts: Swiss FX Trading Platform,” accessed April 28, 2023, https://www.dukascopy.com/swiss/english/about/fee-schedule/trading-commission-discount-program/
46. “What Is Ethereum?,” ethereum.org, accessed March 18, 2023, https://ethereum.org/en/what-is-ethereum/
47. “What You Need to Know about Privacy Coins,” Binance Blog, accessed March 17, 2023, https://www.binance.com/en/blog/fiat/what-you-need-to-know-about-privacy-coins-421499824684903655
48. A. Au et al., “Care, Custody, & Control (CCC): Identification, Quantification, and Mitigation of Cryptocurrency Custodial Risk.,” Cryptocurrency and Cyber Risk: Market Analysis and Perspectives, June 2020.
49. Adam Hayes, “What Is Premining?,” Investopedia, December 30, 2022, https://www.investopedia.com/terms/p/premining.asp
50. Administration fédérale des contributions AFC, “Cryptomonnaies – Fiscalité,”(Cryptocurrencies and initial coin/token offerings (ICO/ITO) as subject to wealth, income and profit tax, withholding tax and stamp duty) AFC, accessed May 2, 2023, https://www.estv.admin.ch/estv/fr/accueil/impot-federal-direct/informations-specialisees-ifd/cryptomonnaies.html
51. Ahmet Burçin YERELİ and Işıl Fulya ORKUNOĞLU-ŞAHİN, “Cryptocurrencies and Taxation,” 5th International Annual Meeting of Sosyoekonomi Society, October 25, 2018.
52. Art, money laundering and terrorist financing: New ... - lalive, accessed May 4, 2023, https://www.lalive.law/data/publications/2015-SGI+DLE-Art,_money_laundering_and_terrorist_financing_new_developments_in_Swiss_law.pdf
53. Blockchain Advocates Push Back After Bolivia Essentially Bans Crypto," CoinDesk, December 4, 2020, https://www.coindesk.com/policy/2020/12/04/bolivia-essentially-banned-crypto-but-blockchain-advocates-are-pushing-back/
54. Calin, “A Brief History of the Amlds: Part Two,” ComplyAdvantage, November 24, 2021, https://complyadvantage.com/insights/brief-history-amlds-part-two/

55. Calin, “History of Anti Money Laundering Directive: A Summary - Part One,” ComplyAdvantage, August 25, 2022, https://complyadvantage.com/insights/brief-history-amlds-part-one/
56. Cambridge Centre for Alternative Finance. "Global Cryptoasset Regulatory Landscape Study." Cambridge Judge Business School, University of Cambridge, April 2019. Available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf.
57. Choo, Kim-Kwang Raymond. “Cryptocurrency and Virtual Currency.” Handbook of Digital Currency, 2015, 283–307. https://doi.org/10.1016/b978-0-12-802117-0.00015-1
58. Circular 2016/7 video and online identification - finma.ch, accessed April 26, 2023, https://www.finma.ch/en/~/media/finma/dokumente/rundschreiben-archiv/2016/rs-16-07/finma-rs-2016-07-20180620.pdf?la=en
59. Clark Sonksen, "Cryptocurrency Regulations in ASEAN, East Asia, & America: To Regulate or Not to Regulate," Washington University Global Studies Law Review 20, no. 1 (2021): 171-200
60. CMS Guide to Employment Issues in an M & a transaction, accessed April 11, 2023, https://cms.law/en/media/local/cms-vep/files/publications/guides/cms-guide-to-employment-issues-in-an-m-a-transaction-2014-3?v=1
61. Cristiano Bellavitis, Christian Fisch, and Johan Wiklund, “A Comprehensive Review of the Global Development of Initial Coin Offerings (ICOS) and Their Regulation,” Journal of Business Venturing Insights, 2021, https://doi.org/10.1016/j.jbvi.2020.e00213
62. Crypto Valley Association, accessed May 10, 2023, https://members.cryptovalley.swiss/
63. D. Towne Morton, "The Future of Cryptocurrency: An Unregulated Instrument in an Increasingly Regulated Global Economy," Loyola University Chicago International Law Review 16, no. 1 (Winter 2020): 129-[ii]
64. Dang, Thu Thuy. "Current Situation of Cryptocurrency in Vietnam." Journal of Business, Economics and Environmental Studies 9, no. 4 (2019): 29-34
65. Danton Bryans, "Bitcoin and Money Laundering: Mining for an Effective Solution," Indiana Law Journal 89, no. 1 (Winter 2014): 441-472
66. Debbie Ward and Bram van Sunder, “How New Rules on Financial Crime Will Impact the EU AML Regime,” EY, September 8, 2021, https://www.ey.com/en_gl/financial-services-emeia/how-new-rules-on-financial-crime-will-impact-the-eu-aml-regime
67. Dirk A. Zetzsche et al., “The ICO Gold Rush: It’s a Scam, It’s a Bubble, It’s a Super Challenge for Regulators,” SSRN Electronic Journal, 2017, https://doi.org/10.2139/ssrn.3072298
68. Eidgenössische Finanzmarktaufsicht FINMA, “Developments in Fintech,” Eidgenössische Finanzmarktaufsicht FINMA, accessed April 24, 2023, https://www.finma.ch/en/documentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/

69. Eidgenössische Finanzmarktaufsicht FINMA, “Finma Ascertains Illegal Activity by Envion AG,” Eidgenössische Finanzmarktaufsicht FINMA, March 27, 2019, https://www.finma.ch/en/news/2019/03/20190327---mm---envion/
70. Eidgenössische Finanzmarktaufsicht FINMA, “Finma Closes down Coin Providers and Issues Warning about Fake Cryptocurrencies,” Eidgenössische Finanzmarktaufsicht FINMA, September 19, 2017, https://www.finma.ch/en/news/2017/09/20170919-mm-coin-anbieter/
71. Eidgenössische Finanzmarktaufsicht FINMA, “Finma Guidance: Stringent Approach to Combating Money Laundering on the Blockchain,” Eidgenössische Finanzmarktaufsicht FINMA, August 26, 2019, https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/
72. Eidgenössische Finanzmarktaufsicht FINMA, “Finma Issues First-Ever Approval for a Stock Exchange and a Central Securities Depository for the Trading of Tokens,” Eidgenössische Finanzmarktaufsicht FINMA, September 10, 2021, https://www.finma.ch/en/news/2021/09/finma-issues-first-ever-approval-for-a-stock-exchange-and-a-central-securities-depository-for-the-trading-of-tokens/.
73. Eidgenössische Finanzmarktaufsicht FINMA, “Money Laundering: Focus of Conduct Supervision (2021),” Eidgenössische Finanzmarktaufsicht FINMA, accessed April 23, 2023, https://www.finma.ch/en/documentation/dossier/dossier-geldwaeschereibekaempfung/geldwaescherei-schwerpunkte-der-verhaltensaufsicht-2021/
74. Eidgenössische Finanzmarktaufsicht FINMA, “Principle-Based Regulation,” Eidgenössische Finanzmarktaufsicht FINMA, accessed May 3, 2023, https://www.finma.ch/en/finma/activities/regulation/
75. Eidgenössische Finanzmarktaufsicht FINMA, “Welcome to the Swiss Financial Market Supervisory Authority Finma,” Eidgenössische Finanzmarktaufsicht FINMA, accessed March 12, 2023, https://www.finma.ch/en/
76. European Central Bank, “For a Few Cryptos More: The Wild West of Crypto Finance,” European Central Bank, April 25, 2022, https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220425~6436006db0.en.html
77. FATF. "Correspondent Banking Services." FATF Recommendations, Financial Action Task Force, 2016, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Correspondent-banking-services.html.
78. FATF. "Guidance on Transparency and Beneficial Ownership." FATF, June 2014, https://www.fatf-gafi.org/content/dam/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.
79. FATF. "Handbook for the Assessment of Vulnerabilities to Money Laundering and Terrorist Financing in the Public Sector - Red Flag Indicators for Virtual Assets." Financial Action Task Force, 2019. Accessed February 8, 2023. https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/Handout-Red-Flags-VA-Public-Sector.pdf.
80. FATF. “Virtual Currencies: Definitions and Potential AML/CFT Risks.” FATF/OECD, June 2014,

https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
81. Federal Office of Police, “Money Laundering Reporting Office Switzerland (MROS),” Startseite, accessed April 26, 2023, https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei.html#:~:text=MROS%20is%20a%20member%20of,money%20laundering%20and%20terrorist%20financing..
82. Federal Tax Administration FTA, “Federal Tax Administration FTA,” EidgenÃ¶ssische Steuerverwaltung - Willkommen, accessed May 4, 2023, https://www.estv.admin.ch/estv/en/home.html#:~:text=rates%20from%202024-,Increase%20in%20VAT%20rates%20from%202024,for%20accommodation%3A%203%2C8%20%25
83. Fedlex, accessed April 29, 2023, https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en
84. Fedlex, accessed April 30, 2023, https://www.fedlex.admin.ch/eli/cc/2015/390/de
85. Fedlex, accessed April 30, 2023, https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en
86. Financial Services Agency, accessed March 14, 2023, https://www.fsa.go.jp/en/
87. Finma guidance 02/2019 - Eidgenössische Finanzmarktaufsicht Finma. Accessed April 11, 2023. https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20190826-finma-aufsichtsmitteilung-02-2019.pdf?la=en
88. Für den Erhalt und Ausbau der Attraktivitat und der Konkurrenzfähigkeit des Blockchain-Standorts Schweiz (To maintain and expand the attractiveness and competitiveness of Switzerland as a blockchain location), Blockchain Federation, accessed May 5, 2023, https://blockchainfederation.ch/?lang=en
89. Galia Kondova and Geremia Simonella, “Blockchain in Startup Financing: Icos and Stos in Switzerland,” SSRN, February 27, 2020, https://deliverypdf.ssrn.com/delivery.php?ID=842027003008098069124116094078007110050040086012039063125106092023100102100088123126100002120123037033111096080122013064124080021011055076033018105079105102010125007028082062115121074109010092090114028022090102087075024110078084105096019073081101094092&EXT=pdf&INDEX=TRUE
90. GBBC Council. (2022). The Global Blockchain Business Council: International Journal of Blockchain Law, Volume II. Retrieved from https://gbbcouncil.org/wp-content/uploads/2022/03/IJBL-Volume-II.pdf.
91. GetMonero. "Monero: secure, private, untraceable." Accessed January 28, 2023. https://www.getmonero.org/.
92. Ghosh, Sharmistha. "Virtual Currency – An Overview." Journal of the Department of Commerce, vol. 4, 2021, pp. 41-50.
93. Global Legal Insights: Blockchain & Cryptocurrency Regulation (S.l.: GLOBAL LEGAL GROUP LTD, 2022).
94. Guidelines - Eidgenössische Finanzmarktaufsicht Finma, accessed April 20, 2023, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en

95. Home, accessed May 1, 2023, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Bpp-finsanctions-tf-r6.html
96. Hughes, Sarah Jane, and Stephen T. Middlebrook. “Regulating Cryptocurrencies In The United States: Current Issues And Future Directions.” Emory Law Journal 68, no. 1 (2018): 195-245.
97. I Cvetkova, “Cryptocurrencies Legal Regulation,” BRICS Law Journal 5, no. 2 (2018): 128–53, https://doi.org/10.21684/2412-2343-2018-5-2-128-153
98. IMF. "Exploring Multilateral Platforms for Cross-Border Payments." Analytical Notes, January 18, 2023. https://www.imf.org/en/Publications/analytical-notes/Issues/2023/01/18/Exploring-Multilateral-Platforms-for-Cross-Border-Payments-528297.
99. International Monetary Fund. "Exploring Multilateral Platforms for Cross-Border Payments." Analytical Notes, January 18, 2023. https://www.imf.org/en/Publications/analytical-notes/Ises/2023/01/18/Exploring-Multilateral-Platforms-for-Cross-Border-Payments-528297.
100. Jia, J., & Wang, W. (2013). Empirical analysis of online forum discussions on Bitcoin. Journal of International Financial Markets, Institutions and Money, 23, 32-44.
101. John Riley, “The Current Status of Cryptocurrency Regulation in China and Its Effect around the World,” China and WTO Review 7, no. 1 (2021): 135–52, https://doi.org/10.14330/cwr.2021.7.1.06
102. Josias N. Dewey, Global Legal Insights: Blockchain & Cryptocurrency Regulation (London: Global Legal Group, 2021).
103. Luis Antonio Ahumada, "An Overview of Blockchain and Distributed Ledger Technologies: Architecture, Operation, and Risks," ECB Working Paper No. 2693 (March 2021), accessed February 27, 2023, https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2693~8d4e580438.en.pdf
104. M. Pravdiuk, “INTERNATIONAL EXPERIENCE OF CRYPTOCURRENCY REGULATION,” Norwegian Journal of Development of the International Science, 2021, https://doi.org/10.24412/3453-9875-2021-53-2-31-37.
105. Manuel Rodriguez, “Operation Rubicon: An Assessment with Regard to Switzerland’s Duties under the Law of Neutrality,” International Journal of Legal Information 50, no. 3 (2022): 82–112, https://doi.org/10.1017/jli.2022.31
106. McGuire, P., and Sushko, V. (2022). "Central bank digital currencies and cross-border payments." Bank for International Settlements Annual Economic Report 2022, chapter 3. Retrieved from https://www.bis.org/publ/arpdf/ar2022e3.htm.
107. Narissa Lyngen, "Basel III: Dynamics of State Implementation," Harvard International Law Journal 53, no. 2 (Summer 2012): 519-536
108. Official Gazette of the Republic of Ecuador, Segundo Suplemento, Año II - Nº 332, Registro Oficial Nº 332, September 12, 2014, https://perma.cc/A69K-7RWU.
109. Olli-Pekka Hilmola, “On Prices of Privacy Coins and Bitcoin,” Journal of Risk and Financial Management 14, no. 8 (2021): 361, https://doi.org/10.3390/jrfm14080361
110. Omri Marian, "A Conceptual Framework for the Regulation of Cryptocurrencies," University of Chicago Law Review Dialogue 82 (2015-2016): 53-68F

111. Payment services act - english - japanese law translation, accessed March 15, 2023, https://www.japaneselawtranslation.go.jp/en/laws/view/3078/en
112. Ranvir Singh Sisodia, "Analysis of Cryptocurrency Laws in India and around the World," Law Essentials Journal 2, no. 1 (2021): 233-239
113. Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism (Washington D.C.: The World Bank, 2006).
114. René Zulauf - Partner, Loris Lipp - Manager, and Thomas Ingold - Assistant Manager, “Swiss Tax Authorities Provide Additional Clarity on Crypto-Taxation,” Tax and Legal blog, accessed May 7, 2023, https://blogs.deloitte.ch/tax/2022/01/swiss-tax-authorities-provide-additional-clarity-on-crypto-taxation.html
115. Russian Government Website, Federal Law of July 31, 2020 No. 259-FZ 'On Digital Financial Assets, Digital Currency, and Amendments to Certain Legislative Acts of the Russian Federation.', Russian Government, July 31, 2020, http://publication.pravo.gov.ru/Document/View/0001202007310056.
116. September 01, Paddy Baker, and CoinDesk, “Tezos Investors Win $25m Settlement in Court Case over $230M ICO,” Nasdaq, accessed May 10, 2023, https://www.nasdaq.com/articles/tezos-investors-win-%2425m-settlement-in-court-case-over-%24230m-ico-2020-09-01#:~:text=A%20lawsuit%20alleging%20the%20Tezos,to%20settle%20the%20case%20Friday
117. Shaen Corbet, Understanding Cryptocurrency Fraud: The Challenges and Headwinds to Regulate Digital Currencies (Berlin: De Gruyter, 2022).
118. SME Portal, “Swiss and European E-Commerce Laws,” Statutory obligations, accessed May 2, 2023, https://www.kmu.admin.ch/kmu/en/home/concrete-know-how/sme-management/e-commerce/creating-own-website/statutory-obligations-in-switzerland-and-the-eu%20.html
119. Stan Higgins, “Ecuador Bans Bitcoin, Plans Own Digital Money,” CoinDesk Latest Headlines RSS, September 11, 2021, https://www.coindesk.com/markets/2014/07/25/ecuador-bans-bitcoin-plans-own-digital-money/
120. State Secretariat for International Finance SIF, “Blockchain / DLT,” Staatssekretariat fÃ¼r internationale Finanzfragen SIF - Startseite, accessed May 3, 2023, https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html
121. State Secretariat for International Finance SIF, “Stablecoins,” Staatssekretariat fÃ¼r internationale Finanzfragen SIF - Startseite, accessed May 6, 2023, https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/stablecoins.html
122. Stephen Turley - Senior Manager and Kristina Bertschinger - Manager, “Cryptocurrencies and Your Swiss Tax Return: Reporting Requirements and Tax Implications,” Tax and Legal blog, accessed May 7, 2023, https://blogs.deloitte.ch/tax/2022/04/cryptocurrencies-and-your-swiss-tax-return-reporting-requirements-and-tax-implications.html

123. Steven Farrugia, Joshua Ellul, and George Azzopardi, “Detection of Illicit Accounts over the Ethereum Blockchain,” Expert Systems with Applications 150 (2020): 113318, https://doi.org/10.1016/j.eswa.2020.113318
124. Szydło, Barbara and Pisarz, Piotr. “Challenges in Regulating Cryptocurrency: A Comparative Analysis of Regulatory Approaches Worldwide.” Journal of Risk and Financial Management 13, no. 9 (2020): 203.
125. Task - admin.ch, accessed April 28, 2023, https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/task.html
126. The Financial Action Task Force (FATF). 2021. “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.” FATF-GAFI, June. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html
127. The Law Library of Congress, Global Legal Research Directorate. "Regulation of Cryptocurrency Around the World: November 2021 Update" (Washington, DC: Library of Congress, 2021)
128. Thi Ngoc Nga Vu, The Impact of Cryptocurrency on Traditional Financial Markets, April 2022, https://www.theseus.fi/bitstream/handle/10024/753871/Vu_Nga.pdf?sequence=2
129. Virtual currency schemes - a further analysis - European Central Bank, accessed April 13, 2023, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
130. Vitelio Brustolin, Dennison de Oliveira, and Alcides Eduardo dos Reis Peron, “Exploring the Relationship between Crypto AG and the CIA in the Use of Rigged Encryption Machines for Espionage in Brazil,” Cambridge Review of International Affairs 36, no. 1 (2020): 54–87, https://doi.org/10.1080/09557571.2020.1842328
131. Walker, Clare and Khawar Qureshi. "Implementing the EU's Fifth Anti-Money Laundering Directive: Challenges and Opportunities." Journal of International Banking Law and Regulation (2019): 468-475.
132. White Paper v. 46 09.02.2023 SL on - dukascoin.com, accessed May 2, 2023, https://www.dukascoin.com/media/White-Paper.pdf?v=10546
133. Wolfsberg Group. "Wolfsberg’s Correspondent Banking Due Diligence Questionnaire (CBDDQ) Glossary." 22 February 2018. Accessed 29 January 2023. https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%27s_CBDDQ_Glossary_220218_v1.0.pdf.
134. Wolters Kluwer, Banking & Financial Services Policy Report 30 (May 5, 2011), https://www.weil.com/~/media/files/pdfs/Basel_III_May_2011.pdf
135. Xie, Rain. "Why China had to 'Ban' Cryptocurrency but the U.S. did not: A Comparative Analysis of Regulations on Crypto-Markets Between the U.S. and China." Washington University Global Studies Law Review 18, no. 2 (2019).
136. Zcash. Accessed January 28, 2023 https://z.cash/.
137. Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. "Regulatory Arbitrage and the Dark Side of Cryptocurrencies." In The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, edited by David Fox, 393-420. Cambridge University Press, 2019.
138. Zhou, Sarah. "Regulating Cryptocurrencies: Assessing Market Reactions." Journal of Applied Corporate Finance 31, no. 2 (2019): 100-108.