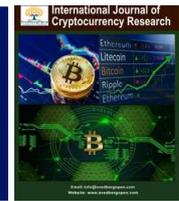




International Journal of Cryptocurrency Research

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

The Implications of Cryptocurrencies on the US BSA/AML Regulation

Kwabena Akyeampong¹  and Robert Munro²

¹Albany Law School, Albany, NY 12208, United States. E-mail: kakyeampong@albanylaw.edu

²Adjunct Professor, Albany Law School, Albany, NY 12208, United States. E-mail: rmunr@albanylaw.edu

Article Info

Volume 5, Issue 2, December 2025

Received : 20 July 2025

Accepted : 27 November 2025

Published : 22 December 2025

[doi: 10.51483/IJCCR.5.2.2025.98-112](https://doi.org/10.51483/IJCCR.5.2.2025.98-112)

Abstract

The study focuses on examining the implications of cryptocurrencies to the Bank Secrecy/Anti-Money Laundering (BSA/AML) framework. Accordingly, it applies a comparative legal research approach to understand trade-offs between cryptocurrencies and BSA/AML through comparing information from different primary sources obtained from LexisNexis, Bloomberg Law, and Westlaw. The motivation behind the study was the rapid adoption of cryptocurrencies among investors and retail consumers, which poses risks to the stability of the financial system. The study noted lack of a devoted prime regulator with paramount powers to oversee all cryptocurrency activities as a gap that blockchain applies, in respect to the regulatory arbitrage theory, to circumvent harsh regulations in some jurisdictions, for favorable ones in other jurisdictions. Some of the features noted to challenge effective regulation of these currencies include anonymity, lack of physical equivalent to bank notes and coins, decentralized, and the agile technology used in blockchain. However, efforts to embrace effective adoption and incorporation of crypto assets into the financial system are being demonstrated through the enactment of House Bills, legislative histories, State and Federal Acts such as the CANSEE) Act (S.2355) to mitigate against the risks of illicit activities perpetrated in the decentralized finance (DeFi). The study established if the current efforts being made might be combined with amendment of the BSA/AML regulation to apply in decentralized finance, identification of a primary regulator for cryptocurrencies, and collaboration between regulators and blockchain developers, they would enhance secure and effective adoption of cryptocurrencies.

Keywords: *Cryptocurrencies, Bank secrecy, Anti-money laundering, Decentralized finance*

© 2025 Kwabena Akyeampong and Robert Munro. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

1. Introduction

The global shifts in the financial services industry have triggered a rising interest in crypto payments among

* Corresponding author: Kwabena Akyeampong, Albany Law School, Albany, NY 12208, United States. E-mail: kakyeampong@albanylaw.edu

2790-1386/© 2025. Kwabena Akyeampong and Robert Munro. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

institutional investors and retail consumers due to the ease of access to virtual currencies, as well as a flexible procedure for conducting and completing peer-to-peer transactions without leaving digital footprints.¹ However, the incorporation of cryptocurrencies into the financial system will trigger the revision of the current BSA/AML framework for effective and optimal mitigation of risks associated with this adoption. This is attributed to the challenges encountered in regulating cryptocurrencies and ensuring their compliance with the current BSA/AML framework. It is essential to ascertain the inherent risks, and tolerable risks associated with the adoption of cryptocurrencies, as well as controls that can mitigate these risks. This leads us to the study's guiding question: what implications does the adoption of cryptocurrencies have on the current BSA/AML framework?

1.1. Background of the Study

Cryptocurrencies have emerged as a preferred means of offering secure and direct payment to online transactions. The novelty of these currencies is in their ability to offer users anonymity to ensure they do not leave footprints after completing transactions. However, malicious actors have previously capitalized on this anonymity to engage in illicit activities such as money laundering, terrorist financing, and tax evasion. The ability of law enforcers to effectively counter these illegal behaviors has been obfuscated by the absence of a primary regulator to oversee the activities of cryptocurrencies, as well as the inability of the current BSA/AML framework to adequately prosecute these criminal behaviors. Cryptocurrencies do not have the physical equivalent of banknotes or coins, and hence, not considered an object of an offense, whose justification beyond a reasonable doubt requires the presence of a movable good.² The fact that the CFTC and SEC have been at the forefront in showing an interest in regulating cryptocurrencies indicates that the future of cryptocurrency regulation is still an open question. On one hand, the SEC has been making aggressive policing of crypto tokens to assume jurisdiction of the crypto network.³ On the other hand, the CFTC has been active in recognizing cryptocurrencies as commodities, a fact that would enable the Internal Revenue Service (IRS) to enforce its Gross Income code and ensure tax compliance among cryptocurrencies. The point of concern halting the success of these efforts is that cryptocurrencies are anonymous, uncertain, and virtual. These elements have been relied upon to justify the exemption of crypto activities from prosecutions whose constituent elements require a movable good.⁴

The legal status of cryptocurrencies remains a point of concern among different regulators. It is not clear whether jurisdictions should explicitly or implicitly regulate cryptocurrencies.⁵ In 2018, the CFTC sued McDonnell for running an illusory and duplicitous cryptocurrency scheme, for purported trading advice, virtual currency purchases and trading, and for embezzling funds belonging to investors.⁶ The case raised concerns about the lack of clarity as to whether the CFTC may regulate cryptocurrencies as a commodity, and whether the Commodity Exchange Act (CEA) amendments under the Dodd-Frank Act may permit the CFTC to exercise its jurisdiction over fraud that does not involve a direct sale of futures or derivatives.

A primary regulator for cryptocurrencies lacks, hence the confusion that exists when different authorities apply their statutes to enforce regulatory requirements to digital transactions. In 2020, Larry Harmon was charged for allegedly enabling users to conceal and obfuscate the source of bitcoins by transmitting them anonymously using Helix, which was considered an unlicensed money-transmitting business.⁷ The Federal Grand Jury in the District of Columbia indicted the defendant for violating Title 18 of US Code 1956 by

¹ Chris Berg, Sinclair Davidson and Jason Potts (2019). Chapter 8: Public Policy in a Blockchain Era. *In Understanding the Blockchain Economy*, Monograph Book, 138-151 (ebook), DOI: <https://doi-org.albanylaw.idm.oclc.org/10.4337/9781788975001.00013>

² Nadja C. Maelle (2019). Chapter 8: Perspectives of a Distributed Future: Aspects of Criminal Law. *In Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law*, Monograph Book, 215-239 (ebook), DOI: <https://doi-org.albanylaw.idm.oclc.org/10.4337/9781788115131.00014>

³ Mark Bini and Joanna Howe (2022). Here's Why the SEC will Likely be the Primary Cryptocurrency Cop. *Bloomberg Law*, October 17. <https://news.bloomberglaw.com/us-law-week/is-the-sec-the-new-crypto-sheriff-in-town>

⁴ *United States v. Payward Ventures, Inc.*, 23-mc-80029.

⁵ Global Legal Research Directorate (2021). Regulation of Cryptocurrency Around the World: November 2021 Update. *The Law Library of Congress*, November. <http://www.law.gov>

⁶ *CFTC v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018).

⁷ *United States v. Harmon*, 474 F. Supp. 3d 76 (D.D.C. 2020).

conspiring to launder monetary instruments.⁸ The case demonstrated an important development in the financial services industry, with some US jurisdictions such as the District of Columbia, already recognizing cryptocurrencies under their Money Transmitters Act, as money. Besides, Financial Crimes Enforcement Network (FinCEN)'s 2013 guideline on the transmission between accounts,⁹ which also qualified as transfer between locations when a virtual currency address is involved, clarified the potential consideration of Helix as a money transmitting exchanger, a fact that made the enforceability of the BSA on registration and compliance to hold. However, the House Bill by Aloupis, as chaptered on December 12, 2022, forms a point of contention concerning the registration requirement for cryptocurrency operators, which was the main reason Larry was indicted, having operated Helix as an unlicensed money transmitter. As a legislative history, the House Bill offers a new definition for virtual currencies that overrides the provision for registration as required by BSA.¹⁰

Tax compliance is an issue associated with cryptocurrency transactions. The IRS is making efforts to ensure crypto transactions are tax-compliant. The Internal Revenue Code has been advanced to recognize gross income as all the income derived from any source, except as the law may exempt. Based on this understanding, the IRS Revenue Ruling 2023-14, affirmed that if a taxpayer uses cash method accounting to stake cryptocurrencies native to a proof-of-stake blockchain and realizes more units of crypto assets as rewards during validation, the rewards received from staking must be included in the income for the tax year in which the taxpayer earns the rewards.¹¹ However, the lack of physical equivalents such as banknotes and coins for cryptocurrencies, makes it hard for the enforcement team to deliberate underreporting of income and tax evasion, as well as determine uncertainties over how to report transactions involving cryptocurrencies.¹²

The Crypto-Asset National Security Enhancement and Enforcement (CANSEE) Act (S.2355), is a legislation enacted to target money laundering, as well as sanction evasion that involves DeFi.¹³ The legislation is meant to end special treatment that the current BSA/AML framework awards DeFi, thus, ensuring crypto operators meet regulatory obligations such as maintaining the AML program, reporting suspicious activities to FinCEN, performing due diligence to customers, and sharing data related to BSA/AML with their subsidiaries across the globe. Additionally, the increasing interest in embracing cryptocurrencies, as well as the need to ensure the stability of the financial system triggered the amendment of the AML Act of 2020 to cover art and antiquities. The goal for the expanded jurisdiction of the AML Act of 2020 was to enforce registration and compliance requirements for the exchange or transmission of products in exchange for money. Accordingly, the new AML Act, like the CANSEE Act (S.2355), overrides the special treatment entitled to crypto assets and related activities. The focus is to minimize the chances of users from engaging in illicit activities such as money laundering, tax evasion, and terrorist financing by providing a close monitoring of crypto activities, thus, restoring sanity in the financial system

1.2. Methodology Statement

Legal research methodology, whose choice relies on the context of the investigation, facilitates attainment of the primary objective. By definition, a methodology is an approach that the researcher employs to conduct a study.¹⁴ Legal research utilizes three methodologies: Doctrinal legal research; empirical methodology; and the comparative approach.¹⁵

Doctrinal legal research, also called "black letter" methodology, focuses on the letter of the law, as opposed to the law in action. The applicability of this methodology is in studies that require composition of a detailed description and analysis of legal rules. The focus is on collecting, organizing, and describing the law to establish an underlying connection between the sources of a particular doctrine. The researcher identifies ambiguities and criticisms of the law to provide solutions. A doctrinal legal research methodology is

⁸ See 18 U.S.C. § 1956(h).

⁹ See FIN-2013-G001.

¹⁰ See Subsections (14), (21), (23), (29), and (35) of section 560.103, Florida Statutes.

¹¹ See 26 CFR 1.61-1.

¹² *United States v. Payward Ventures, Inc.*

¹³ See CANSEE Act (S.2355).

¹⁴ Chunuram Soren and Sudhansu Ranjan Mohapatra (2021). Legal Research Methodology: An Overview, *Journal of Emerging Technologies and Innovative Research*, 10, 442-483.

¹⁵ Mark van Hoecke (2013). Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?.

advantageous when providing a solid structure for crafting, organizing a study, and facilitating a comprehensive definition and explanation of the rule. However, it tends to be too formalistic, thus, oversimplifying the legal doctrine.¹⁶ Since the study focuses on the implications of cryptocurrencies on the U.S BSA/ AML regulation, rather than the wording of the BSA/ AML framework, the doctrinal legal research is not adequate to facilitate the realization of the study's objective.

The empirical approach, as a legal research methodology, uses data analysis to investigate legal systems.¹⁷ This approach is executed in four steps: project design; data collection and coding; data analysis; and result presentation. Two main types of empirical legal research are: quantitative and qualitative. Quantitative, also known as numerical empirical legal research, involves the acquisition of information about cases and court rulings, and translating that information into numerals for effective analysis using appropriate statistical tools such as SPSS, STATA, and Python. An advantage of this method is that it only deals with facts and verifiable information, hence, useful in making informed decisions that reflect the prevailing phenomenon. However, it suffers drawbacks such as being limited to numbers only, and vulnerable to subjective interpretation, as well as intentional manipulation, thus, not suitable for the current study. The qualitative, also known as non-numerical empirical legal research method, focuses on the extraction of information from legal documents. The researcher interprets and categorizes the extracted information into themes for identification of patterns. Although this approach is useful in education research due to its ability to facilitate a deeper understanding of a contextual phenomenon, it is subject to personal experience and knowledge,¹⁸ which may influence observations and conclusions made from a study, thus, not suitable for this research.

The comparative legal research approach focuses on critical analysis of different bodies of the law to assess how the outcome of a legal proceeding could vary under different sets of laws.¹⁹ This approach allows the researcher to perform comparisons between different regulatory authorities such as the regulation of cryptocurrencies under CFTC as commodities, and regulation of the same currencies under SEC as securities to ascertain a jurisdiction that may be more adequate to maintain the sanity and stability of the financial system after the adoption of cryptocurrencies. The adoption of this approach will help the researcher to establish a common ground between different case texts, American Law Reports, information from U.S Law Week Articles, and State or Federal legislative history for understanding the trade-offs between cryptocurrencies and BSA/ AML regulation. Accordingly, it will help uncover potential implications that the adoption of cryptocurrencies may have to the current BSA/ AML framework, thus, facilitating the development of robust amendments that may enhance the framework to ensure effective regulation of cryptocurrencies. Although this approach suffers a shortcoming in obtaining materials from other jurisdictions,²⁰ the researcher will use primary sources that include LexisNexis, Bloomberg Law, and Westlaw to acquire adequate materials about the area of interest to help generate knowledge that will arguably facilitate the development of analytical and thinkable thoughts about BSA/ AML and a critical understanding of how the current BSA/ AML framework can be strategically enhanced to adequately regulate cryptocurrencies.

1.3. Theoretical Perspective

The study aligns with the Regulatory Arbitrage Theory, in the sense that participants in the crypto environment continue to exploit inconsistencies and loopholes in the current regulatory framework to their advantage.²¹ The US is yet to agree on the primary regulator of cryptocurrencies. Particularly, it is not clear whether cryptocurrencies should be regulated as commodities under CFTC, or as securities under SEC. The absence of a primary regulator for these currencies, which continue to evolve due to technological agility, has become a puzzle to many US states on how effectively crypto assets may be regulated.

¹⁶ Gaurav Shukla (2023). Doctrinal Legal Research: A Library-based Research.

¹⁷ Lee Epstein and Andrew D. Martin (2014). An Introduction to Empirical Legal Research.

¹⁸ Nadia E. Nedzel (2004). Legal Reasoning, Research, and Writing for International Graduate Students.

¹⁹ Marie-Luce Paris (2016). The Comparative Method in Legal Research: The Art of Justifying Choices.

²⁰ Edward J. Eberle (2011). The Mythology of Comparative Law.

²¹ Jan Friedrich and Matthias Thiemann (2020). The Economic, Legal and Social Dimensions of Regulatory Arbitrage. December 8.

The existing regulatory fragmentation across US jurisdictions subject cryptocurrencies to a patch of regulations, with each State trying to adopt different rules to mitigate against the risks that crypto assets. However, these efforts, although positive as they may seem, unknowingly, create opportunities for regulatory arbitrage.²² The corporate practice of utilizing favorable regulations in one jurisdiction to circumvent less favorable ones in other jurisdictions has become a norm among cryptocurrency participants, thus, promoting regulatory arbitrage.²³ From this theoretical perspective, cryptocurrencies continue to introduce complexities that favor arbitrage in the financial regulatory environment.²⁴ The anonymous and decentralized nature of crypto assets, together with the evolving technology, challenge the capacity of the current BSA/AML framework to effectively regulate activities carried out in the crypto environment.

The current inconsistencies and loopholes in the current BSA/AML framework requires a multi-faceted approach to handle, including collaboration among US jurisdictions through the adoption of a uniform law for cryptocurrencies, regulatory adaptation to respond effectively to changes in the crypto environment, and a strive towards regulatory consistency to curb special treatment that virtual currencies enjoy, which in essence, create opportunities for regulatory arbitrage.

1.4. Organization of the Thesis

The study is organized into nine logical, and coherent sections. The first section is the abstract of the study, offering the reader a quick preview of the study's purpose, relevance of the study, and the major outcomes. The second section is the introduction, stating the primary research question, background, and methodology statement. The third section is the historical background, setting the stage for describing the sociohistorical relevance of cryptocurrencies to BSA/AML regulation. The fourth section is the literature review, examining the critical works in cryptocurrency and BSA/AML regulation, gaps in the research, and how the study fills the identified gaps. The fifth section discusses the major findings of the study. The remaining sections include the conclusions that summarize the entire study, recommendations, future areas of research, and a bibliography that lists all the sources used in the study.

2. Historical Background

2.1. History of Cryptocurrency

2.1.1. The Idea Behind Cryptocurrency and the Invention of Bitcoin (1982-2010)

The history of cryptocurrencies dates back to 1982's publication by Chaum on "Computer systems established, maintained, and trusted by mutually suspicious groups." The publication laid a foundation for future transformation in blockchain technology.²⁵ Chaum invented the "blinding formula" for sending and receiving tokens without a central authority.²⁶ In the 1990s, Chaum released "eCash" through DigiCash, triggering the attention of enterprises such as Microsoft, but only to run out of funds by 1998.²⁷ More developers emerged in blockchain technology and used Chaum's experiment to create digital tokens such as EGold and Bit Gold that would imitate the price stability of gold.²⁸ These tokens did not succeed, but influenced Satoshi Nakamoto to invent Bitcoin between 2008-2010.²⁹ Bitcoin used proof-of-work as a consensus mechanism to validate transactions on the network, an approach that transformed it into a revolutionary currency and a household name in the crypto environment. Bitcoin development was a fascinating move in the cryptographic space. However, it did not attract the attention of the mainstream financial industry due to the absence of big crypto exchanges, and the fact that information about crypto assets was still scarce on the internet.

²² Katja Langenbucher (2020). Regulatory Arbitrage: What's Law Got to Do with It?. July 16.

²³ Annelise Riles (2014). Managing Regulatory Arbitrage: A Conflict of Laws Approach. *Cornell International Law Journal*.

²⁴ Burcu Hacibedel and Hector Perez-Saiz (2023). Assessing Macro-financial Risks from Crypto Assets. *International Monetary Fund*, 214. <https://doi.org/10.5089/9798400255083.001>

²⁵ Nikolett Antal-Molnar (2022). The Evolution of the Digital Currency. *IJCBE*, 3(1), 1-11.

²⁶ Chaum (1983). Blind Signature for Untraceable Payments. In Chaum D., *Advances in Cryptology*, 199-203.

²⁷ Rice Bogarat (2018). A Very Brief History of Blockchain Technology Everyone Should Read. *Forrás*. <https://ripple.com/insights/needham-report-welcome-to-the-internet-of-value/>

²⁸ Benjamin Masama and JP Bruwer (2021). The Feasibility of Blockchain Technology as a Tool for Zimbabwean Financial Inclusion: An Online Desktop Review. *Social Science Research Network*.

²⁹ Somogyvári Bugár (2020). Bitcoin: Digital Illusion or a Currency of the Future?. *Financial and Economic Review*, 132-153.

2.1.2. *The Growth of Crypto Market (2010-2014)*

Bitcoin traded around \$1 per coin till 2010, before experiencing a pump in 2011 after featuring in Forbes, realizing a high of \$9 per coin.³⁰ However, the price increase did not facilitate Bitcoin's acceptance and adoption since there were allegations that the pseudonymity of the coin promoted criminal activities. Accordingly, the Bitcoin community created a not-for-profit Bitcoin Foundation in 2012 and published Bitcoin Magazine to trigger mainstream attention.³¹ The efforts led to the creation of altcoins, which although are no longer prominent, led to the creation of Litecoins and Ripple's XRP, which are still traded heavily.

2.1.3. *Security Development and the Rise of the Ethereum Network (2014-2016)*

The crypto industry suffered a major security breach after hackers stole 850,000 BTC from the Mt. Gox exchange, making users to question the security of the coin. [32] However, the setback helped crypto supporters to develop secure crypto exchanges (CEXs) that offered insurance protection to investors, a practice that is still embraced by Binance and Coinbase, which are among the major crypto exchanges. In 2015, Ethereum developers came up with a network that would decentralize the Internet, rather than being a payment system or a store of value.³³ The development introduced smart contracts for fulfilling commands using codes once the set conditions were met and led to the development of Non-Fungible Tokens (NFT) and Decentralized Finance (DeFi). As the world's second-largest cryptocurrency, most projects adopted the Ethereum protocol in their decentralized applications, only for the network to suffer the 2016 severe hack in the Decentralized Autonomous Organization (DAO), which was operating as an investment vehicle, causing a \$60 million loss from the \$150 million fund.³⁴ Handling the loss triggered mixed reactions among the Ethereum community, with a section of members supporting the need to return the funds by "forking" the existing network into a new Ethereum, whereas others supporting the need to keep the original Ethereum, arguing that true DeFi needed no human intervention.³⁵ Eventually, the community opted for the "fork" approach, which became influential up-to-date.

2.1.4. *The Popularity of Cryptocurrency (2018-Date)*

The period between 2016 and 2017 experienced a hike in the price of Bitcoins, soaring through \$10,000, and reaching \$20,000,³⁶ before experiencing a "crypto winter" that extended till 2019. During the same period, the Ethereum ecosystem experienced significant transformations, with NFT emerging as a unique digital collectible. However, it was until 2020 that the crypto market gained more attention, with Bitcoin topping at almost \$70,000 per coin.³⁷ Enterprises such as MicroStrategy and Tesla began recognizing the coin as a currency, with El Salvador embracing it as a legal tender. Between 2021 and 2022, the crypto market suffered a major setback after TerraForm Labs' US Stablecoin declined to zero, dragging down Crypto entities and centralized lending platforms tied to the coin.³⁸ Nonetheless, the crypto market managed to retain its \$1 trillion market cap in 2022, thus, attracting attention from central regulators, including SEC and CFTC.

2.1.5. *Regulatory Interest in Cryptocurrencies*

The current BSA/AML framework has been limited in its ability to regulate cryptocurrencies, which are decentralized, virtual, anonymous, and lack a physical equivalent of bank notes or coins that would make them a movable good.³⁹ The risks associated with the pseudonymity of crypto assets, have triggered regulatory interest in overseeing activities of the virtual environment to minimize potential engagement in illicit activities

³⁰ Sornette Huber (2020). Boom, Bust, and Bitcoin: Bitcoin-Bubbles as Innovation, Swiss Finance Institute Research Paper No. 20-41, 1-25.

³¹ Sornette Huber, at 15.

³² Parikshit Mishra (2023). Infamously Hacked Crypto Exchange Mt. Gox Delays Repayment Deadline by a Year, *CoinDesk*, September 21. <https://www.coindesk.com/business/2023/09/21/mt-gox-pushes-repayments-by-a-year/>

³³ Matt Levine (2022). The Only Crypto Story You Need. *Bloomberg*, October 25. <https://www.bloomberg.com/features/2022-the-crypto-story/>

³⁴ David Z. Morris (2023). How the DAO Hack Changed Ethereum and Crypto. *CoinDesk*, May 9.

³⁵ Alyssa Hertig (2016). Ethereum's Two Ethereum Explained. *CoinDesk*, July 28.

³⁶ Statista (2023). Bitcoin (BTC) Price per Day from April 2013-November 16. <https://www.statista.com/statistics/326707/bitcoin-price-index/>

³⁷ Statista (2023).

³⁸ *Id.*

³⁹ Davitian Law, P.A. (2022). The Bank Secrecy Act and Cryptocurrency, *Cryptocurrency Cases*. <https://davitianlaw.com/cryptocurrency-defense/bank-secrecy-act/>

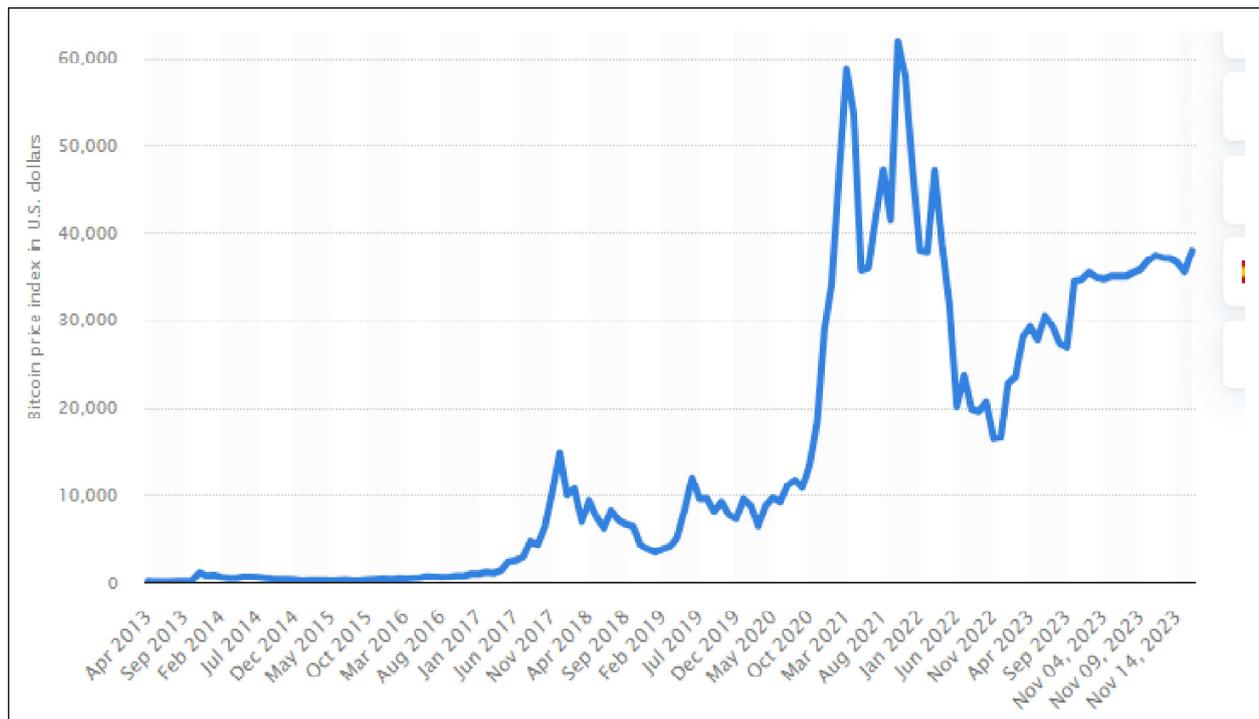


Figure 1: BTC Price History from April 2013 to November 16, 2023

Source: Statista.

such as money laundering, transaction concealment to evade tax, and terrorist financing. Accordingly, the US President issued an Executive Order (EO) in March 2022, detailing comprehensive plans to develop a framework for regulating cryptocurrencies.⁴⁰ The EO succeeded a November 2021 report from the President's Working Group on Financial Markets, which suggested the need to impose bank regulations on stablecoin issuers. The report corresponded with the Office of Foreign Assets Control (OFAC)'s launch of a new set of guidelines on cryptocurrencies for financial sector compliance teams in October 2021.

The government issued a comprehensive proposal on regulating crypto assets in June 2022 under the Lummiss-Gillibrand Bill or the Responsible Financial Innovation Act. The Bill addresses the jurisdiction of SEC and CFTC, tax treatment of digital assets, regulation of stablecoin, and interagency coordination.⁴¹ The Bill was triggered by the shifting global AML landscape and technological innovation that continually prompted the need for regulators and the financial industry to ensure proactiveness in their flexibility to operate within the dynamic cryptographic space. However, the effectiveness of this Bill and other legislations focused on ensuring secure and effective adoption of cryptocurrencies in the financial industry relies on innovative partnerships between regulators and financial institutions, and collaboration with global States to develop reasonably suitable AML amendments for this purpose.

3. Literature Review

3.1. Transformations in Cryptocurrency Regulation

The academic and regulatory communities continuously develop an intensive interest in the implications of cryptocurrencies on the BSA/AML regulation. This is attributed to the dynamic nature of blockchain technology, whose features that include anonymity of transactions, privacy of data, and decentralized operations have triggered global shifts in the financial services industry, leading to an increase in the demand for digital payments among investors and retail consumers.⁴² The need to maintain sanity and integrity of the financial system, in the face of the dynamic decentralized finance has been a basis for continued prosecutions and

⁴⁰ S The Lummiss-Gillibrand Responsible Financial Innovation Act (S.4356).

⁴¹ *Id.*

⁴² Chris Berg, Sinclair Davidson and Jason Potts (2019). *Understanding the Blockchain Economy*, 145.

legislations to reinforce the current BSA/ AML regulation in a bid to seal existing gaps in the current framework that malicious actors might capitalized on to commit financial crimes.⁴³

Scholars in virtual economies and financial crimes, such as Shima Keene examined emerging threats in the virtual environment, with a kin reference to financial crimes, and an extensive clarification of the criminal elements of the virtual world that impact the real world.⁴⁴ According to Keene, the absence of a strong regulation to govern the virtual environment contributes to an increase in financial crimes in this environment, which offers special treatment to users, who execute their illicit activities without the fear of detection or prosecution.⁴⁵ Chambers-Jones Claire underscored this finding by analyzing how the development of Web 3.0 promote the use of digital wallets to execute privately and anonymously, illicit activities such as wash trading, terrorist financing, code exploits, and money laundering.⁴⁶ In another independent investigation, Chambers-Jones Claire and Henry Hillman delved into financial indicators that may help business entities that engage in cryptocurrency exchanges to identify and report criminal behavior perpetrated through the use of cryptocurrencies.⁴⁷ The two scholars noted the anonymity that cryptocurrencies offer as a motivation towards criminal behavior among users.

The regulation of cryptocurrencies remains a concern due to the lack of a primary regulator assigned to fully oversee cryptographic activities in the blockchain environment. Katherine A. Lemire's report on cryptocurrency and anti-money laundering enforcement offers a glimpse of the various regulators involved in regulating cryptocurrencies such as FinCEN, SEC, CFTC, and State regulators.⁴⁸ The Global Legal Research Directorate highlights the regulation of cryptocurrency around the world.⁴⁹ The report focuses on the legal status of cryptocurrencies by evaluating whether a jurisdiction should explicitly or implicitly ban cryptocurrencies. Implicit bans are defined as the prohibition of banks from dealing in cryptocurrencies or offering services to individuals who deal in cryptocurrencies. The report provides insights into the application of tax laws, anti-money laundering, and counter-financing of terrorism to cryptocurrencies. However, the BSA/AML framework is currently limited in its application, whereby it is only enforceable to transactions involving currency exchangers.⁵⁰

The recent past has seen several case proceedings and prosecutions against crypto users and providers who engage in illicit activities. *In re* United States v. Payward Ventures, Inc., the IRS summoned Payward Ventures Inc., and its subsidiaries for operating Kraken, an online cryptocurrency exchange platform for customer information with a belief that the platform could obtain identifying details about its users.⁵¹ However, the court denied the IRS's request to pursue broader details about the platform such as customers' net worth. In the matter of CFTC v. McDonnell, in which CFTC sued McDonnell for operating a deceptive and fraudulent virtual currency scheme, for purported virtual currency trading advice, purchase and trading of cryptocurrencies, and misappropriation of investors' funds, the jurisdiction authority of CFTC was questioned. At the outset of the litigation, the primary concern raised was whether CFTC had a standing to legally sue McDonnell, or assumed that the defendant had violated CEA.⁵² The court granted injunctive relief to the plaintiff after establishing that the defendant had committed fraud by misappropriating investors' funds and committing misrepresentation by providing false advice and promising future returns.⁵³ Based on the court's

⁴³ Nadja C. Maelle (2019). Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law, 225.

⁴⁴ Shima Keene (2011). Emerging Threats: Financial Crime in the Virtual World. *Journal of Money Laundering Control*, 15(1), 25-37 (ebook). DOI: 10.1108/13685201211194718

⁴⁵ Shima Keene, Emerging Threats: Financial Crime in the Virtual World.

⁴⁶ Chambers-Jones Claire (2012). Chapter 5: A Real Crime in a Virtual World. *In Virtual Economies and Financial Crime*, Monograph Book. DOI: <https://doi-org.albanylaw.idm.oclc.org/10.4337/9781849809337.00012>

⁴⁷ Chambers-Jones Claire and Henry Hillman (2014). Chapter 6: Digital Currencies and Financial Crime. *In Financial Crime and Gambling in a Virtual World*, Monograph Book, 137-165 (ebook). DOI: <https://doi-org.albanylaw.idm.oclc.org/10.4337/9781782545200.00012>

⁴⁸ Katherine A. Lemire (2022). Cryptocurrency and Anti-Money Laundering Enforcement. *Reuters*, September 26. <https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/>

⁴⁹ Global Legal Research Directorate. *The Law Library of Congress* (November, 2021).

⁵⁰ BSA/AML Framework is currently limited in the sense that it does not apply to transactions that are meant to facilitate own purposes, but only to transactions that are executed to benefit others.

⁵¹ *Id.*

⁵² 7 U.S.C 1, *et seq.*

⁵³ CFTC v. McDonnell.

ruling, the CFTC had regulatory jurisdiction over several markets engaging in futures and derivatives. However, there was no clarification as to whether virtual currencies were classified as commodities or not.

The United States, *in re* US v. Harmon, sued the defendant for allegedly operating an underground tumbler for Bitcoins, in which the platform facilitated anonymous transactions for clients to conceal and obfuscate the source or owner of the crypto assets. The Federal Grand Jury in the District of Columbia indicted the defendant for violating Title 18 of the US Code 1956 by conspiring to launder monetary instruments.⁵⁴ The case demonstrated an important development in the financial services industry, with some US jurisdictions such as the District of Columbia recognizing cryptocurrencies under their Money Transmitters Act, as money. Besides, FinCEN's 2013 guideline on the transmission between accounts, which also qualifies as transfer between locations when a virtual currency address is involved, clarified the potential consideration of Helix as a money transmitting exchanger, a fact that makes the enforceability of the BSA on registration and compliance of crypto exchanges and providers to hold. However, the absence of a primary regulator of cryptocurrencies halts the implementation of this merit. In another legal matter, US v. Coinbase, the US petitioned to enforce IRS summons served to Coinbase, Inc., under Subchapter A of Title 26 of the US Code 7401-7420.⁵⁵ In this proceeding, the IRS narrowed its summons to obtain information about Coinbase customers with at least the equivalent of \$20,000 in any single transaction type in any one year between 2013 and 2015.⁵⁶ However, intervenors repressed the summons, noting that the records of customers in the picture, were not covered under the narrowed summons. In another separate proceeding, United States v. Approximately 32133.63 Tether (USDT) Cryptocurrency from Binance Account No. Ending in 8770, 1:22-cv-989, the US filed a complaint for *in rem* civil forfeiture, Dkt. No. 1, leading to the execution of a warrant of arrest that saw the defendant's property confiscated. Dkt. No.7. The plaintiff alleged that the defendant handed over, besides store and target gift cards, 0.42203632 Bitcoins, equivalent to 8,926.23 USDT, allegedly associated with the Binance account number ending in 8770.⁵⁷ However, the US failed to demonstrate satisfactorily, how the alleged amount could be traced to the said Binance account number.

The Office of Attorney General and the Department of Justice have been proactive in enforcing legal measures against fraud perpetrated through cryptocurrencies. On November 7, 2022, the Attorney General's office announced a historic 3.36 billion cryptocurrency seizure and conviction related to Silk Road Dark web fraud.⁵⁸ As the second largest seizure in the history of the Department of Justice, the maximum potential sentence for that case was to be prescribed by Congress, with the prosecution being overseen by the Office's Money Laundering and Transactional Criminal Enterprises Unit. In another incident, the Department of Justice reported arresting two suspects for alleged conspiracy to launder \$4.5 billion in stolen cryptocurrency, directly linked to the 2016 hack of DAO.⁵⁹ According to the Deputy Attorney General Monaco's remarks, the current AML framework is effective in preventing criminals from finding a haven in the cryptographic space to execute their illicit activities. Although the crime was based on digital anonymity, the law enforcers from the Department of Justice uncovered the chain that the laundered money took.

SEC and CFTC are the notable authorities recently noted with an intense interest in regulating cryptocurrencies. SEC has engaged in aggressive policing of crypto tokens to assume jurisdiction of the crypto network.⁶⁰ According to the SEC chair, Gary Gensler, digital tokens constitute securities, a fact that triggers the need for crypto intermediaries to register their respective functions with the SEC before engaging in crypto securities transactions. This registration includes both centralized and decentralized intermediaries since

⁵⁴ *See Id.*

⁵⁵ 26 U.S.C. §§ 7402(b) and 7604(a).

⁵⁶ United States v. Coinbase, Inc., 3: 17-cv-01431.

⁵⁷ United States v. Approximately 32133.63 Tether (USDT) Cryptocurrency from Binance Account No. Ending in 8770, 1:22-cv-989.

⁵⁸ US Attorney's Office (2022). US Attorney Announces Historic 3.36 billion Cryptocurrency Seizure and Conviction in Connection with Silk Road Dark Web Fraud. *Press Release*, November 7. <https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction>

⁵⁹ Department of Justice (2022). Two Arrested for Alleged Conspiracy to Launder \$4.5 billion in Stolen Cryptocurrency. *Press Release*, February 8. <https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency>

⁶⁰ Mark Bini (2022). Joanna Howe. *Bloomberg Law*, October 17.

they use non-discretionary methods to match orders of buyers and sellers of crypto securities tokens and, thus, meet the regulatory criteria for being securities exchanges. On the other hand, the CFTC has been active in recognizing cryptocurrencies as commodities, a fact that would enable the IRS to enforce its Gross Income code and ensure tax compliance among cryptocurrencies. The recognition of Bitcoins as commodities has critical implications for the legal authority, between CFTC and SEC that can effectively regulate virtual currencies while ensuring they do not destabilize the current financial system through illicit activities. The fact that virtual currencies are equated to commodities such as agricultural products, overrides their existence in the virtual environment, not forgetting that unlike the SEC, which has broader regulatory powers over securities trading, the CFTC does not have such broader powers over spot trading.⁶¹ Based on this, recognizing virtual currencies as commodities may create more gaps that might be used to commit illicit activities because as a commodity, once an individual takes custody of his/her crypto assets, that individual will not be coerced into trusting an exchange or an intermediary to transact the commodities, but complete transactions through Peer-2-Peer.⁶² Although both efforts from the two regulators are feasible if implemented, cryptocurrencies are anonymous, uncertain, and virtual, hence, exempted from prosecutions whose constituent elements require a movable good.⁶³

The absence of clarity about the primary regulator of cryptocurrencies, as well as the need to align and embrace the increasing demand for the adoption of cryptocurrency has motivated State and Federal authorities to develop different regulations and legislations to mitigate against the negative impacts that may arise from the incorporation of cryptocurrencies into the financial system. The Crypto-Asset National Security Enhancement and Enforcement (CANSEE) Act (S.2355) is a legislation focused on reinforcing the BSA/AML. It targets money laundering and sanctions evasion perpetrated through the virtual environment. The legislation is meant to end special treatment that the current BSA/AML framework awards DeFi, thus, ensuring crypto operators meet regulatory obligations such as maintaining the AML program, reporting suspicious activities to FinCEN, performing due diligence to customers, and sharing data related to BSA/AML with their subsidiaries across the globe. In addition to this Act, several House and Senate Bills have been enacted to ensure effective adoption of cryptocurrencies. The Colorado Senate Bill 22-025, coded as 2022 CO S.B.25(NS), is focused on helping the State treasurer of Colorado to evaluate the feasibility of using security token offerings for State financing and ascertain the degree to which the use of these tokens may facilitate the realization of the State's best interests.⁶⁴ Florida House Bill No. 273, creates a new definition for virtual currencies and eliminates a requirement that crypto sellers must have a Sunshine State money transmission license to operate.⁶⁵ The Bill defines virtual currency as a medium of exchange in electronic or digital format that is not currency. However, it excludes a medium of exchange in electronic or digital format that is issued by, or on behalf of a publisher and used solely within an online game, game platform, or family of games sold by the same publisher, or offered in the same game platform; or that which is used exclusively as part of a consumer affinity or reward program and can be applied solely as payment for purchases with the issuer or other designated merchants, but cannot be converted or redeemed for currency or another medium of exchange.⁶⁶ This House Bill makes it possible for the maintenance of transaction records involving virtual currencies to prevent their use in criminal activities.

Idaho House Bill No. 583, focuses on amending Title 28, of the Idaho Code, by adding Chapter 53 to help define the legal status of crypto assets and the applicability of laws or rules that are related to their business activity.⁶⁷ Chapter 53 of Title 28, Idaho Code,⁶⁸ subjects the purchase or sale of crypto assets to similar laws that apply to other personal property. It facilitates the identification of a purchaser or seller of crypto assets in any way, including by name, identifying number, private key, account number, or office number. Thus, it eliminates the anonymity associated with the crypto environment, which has been making the prevention of illicit activities

⁶¹ Rober Stevens (2023). Securities vs. Commodities: Why it Matters in the Crypto Market. *Coindesk*, May 5.

⁶² Wayne Duggan and Micheal Adams (2023). How Does the SEC Regulate Crypto. *Forbes*, June 30.

⁶³ *Id.*

⁶⁴ See Section 2. In Colorado Revised Statutes, add 24-36-121.5.

⁶⁵ See *Id.*

⁶⁶ 2022 FL H.B. 273 (NS).

⁶⁷ 2022 ID H.B. 583 (NS).

⁶⁸ 28-5305, Idaho Code.

executed anonymously arduous. Virginia House Bill No. 263, is focused on enabling banks and other financial institutions in the State of Virginia to provide customers with crypto custody services.⁶⁹ The General Assembly of Virginia added section 6.2-818.1 into Article 2 of Chapter 8 of Title 6.2,⁷⁰ to accommodate virtual currencies into the current laws applicable to custody services. Paragraph B of the new section requires banks to implement risk management systems and controls that are reasonably designed to effectively monitor, measure, and control risks associated with the custody of crypto assets. Another legislation is the Louisiana House Bill No. 802, which allows financial institutions and trust companies to serve as custodians of crypto assets. As revised under Chapter 22 of Title 6 of the Louisiana Revised Statutes of 1950, to be comprised of R.S 6: 1402,⁷¹ trust companies and financial institutions will serve as custodians of crypto assets after self-assessing themselves and establishing appropriate protocols and risk management controls to mitigate against potential risks associated with offering these services.

3.2. Research Gap

A critical gap in the literature lies in the examination of practical challenges that regulators face in enforcing the BSA/AML framework to cryptocurrencies. There is no primary regulator responsible for overseeing activities of virtual currencies. Also, cryptocurrencies lack a physical equivalent to fiat currencies to be considered an object of offense in proceedings that need the elements of a movable good. In this understanding, the decentralized and cross-border nature of cryptocurrency transactions require a proper understanding of regulatory strategies that need to be incorporated into the current BSA/AML framework to combat financial crimes perpetrated in the cryptographic space.

3.3. Filling the Gap

The study offers a systematic analysis of the real-world implications of cryptocurrencies on the BSA/AML framework, through an in-depth exploration of recent regulatory developments, case texts, and technological advancements to understand the dynamic nature of cryptocurrencies and the evolving challenges that regulatory bodies face in enforcing the law to cryptocurrencies. It proposes adaptive solutions that may be incorporated into the current BSA/AML regulation for safe and effective adoption and incorporation of cryptocurrencies into the financial system.

4. Discussion

The emergency of digital currencies poses multifaceted implications that include challenges and opportunities to financial regulators. The massive adoption of digital currencies raises essential considerations that regulators need to factor in the current BSA/AML framework for effective regulation of these currencies while ensuring the stability and sanity of the financial system. This section presents a discussion of various implications that the adoption of digital currencies into the current financial system pose to the US BSA/AML regulation.

4.1. Customer Due Diligence (CDD)

The pseudonymity feature of the digital world allows users to engage in transactions without leaving behind audit trails.⁷² This anonymity makes it hard for financial regulators to understand the real-world users behind wallet addresses. From the dimensions of the Regulatory Arbitrage principle, malicious actors behind anonymous addresses capitalize on this gap to engage in illicit activities without the possibility of being noticed. Accordingly, the adoption of digital currencies implies that regulators need to enhance customer due diligence requirements for providers of digital wallets. Based on the existing literature, the CDD Final Rule requires reporting entities to comply with CDD requirements by collecting specific data about their customers during the Know Your Customer (KYC) procedure.⁷³ However, applying this provision to crypto exchanges

⁶⁹ 2022 VA H.B. 263 (NS).

⁷⁰ § 6.2-818.1.

⁷¹ 2022 LA H.B. 802 (NS).

⁷² *Id.*

⁷³ FinCEN (2020). Information on Complying with the Customer Due Diligence (CDD). *Final Rule*, August. <https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule>

and wallet providers is yet to be effective. This has been attributed to the lack of a fiat equivalency to cryptocurrencies for effective enforcement of the BSA/AML regulations to cryptocurrencies.⁷⁴ The BSA/AML regulation need to be enhanced to adapt CDD requirements even in the case of pseudonymous transactions. This implication goes hand in hand with CANSEE Act (S.2355), which is focused on ending special treatment of virtual currencies to ensure crypto exchanges and wallet address providers meet regulatory obligations that include maintaining the AML program, reporting suspicious activities to FinCEN, performing due diligence to customers, and sharing customer data with regulators as may be deemed appropriate.

The crypto space is in itself transparent due to the use of blockchain.⁷⁵ Moody's analytics, an economic risk, performance, and financial modeling research entity, indicated that digital ledgers capture each transaction to facilitate tracking back of crypto transactions to a wallet address.⁷⁶ However, connecting the wallet address to the user is something that challenges regulators. Although cryptocurrency exchanges and wallet address providers have continuously subjected users to accurate and perpetual KYC procedures that include the collection of biometric data, the pseudonym feature is pivotal in attracting malicious actors towards using crypto wallets as a vehicle for stealing funds and evading sanctions, as evident in Chainalysis's report, a blockchain analytics firm that reported an increase in illicit use of cryptocurrencies, hitting a higher record of \$20.1 billion in 2022.⁷⁷ The anonymity feature is underscored by the decentralized and distributed nature of cryptocurrencies to make tracing of transactions by financial regulators more challenging. Thus, amending the BSA/AML regulations to adequately apply to cryptocurrencies will enhance the required transparency that include connecting real-world users to specific wallet addresses even if the transactions are executed anonymously.

4.2. Incorporation of Blockchain Analytics and Smart Contracts into BSA/AML Framework

Cryptocurrencies operate in a decentralized environment, with no central authority such as central banks to offer oversight to transactions.⁷⁸ The absence of a central authority is advantageous to malicious actors since it makes it difficult for financial regulators to apply conventional regulatory controls to cryptocurrencies.⁷⁹ Based on GAO report to Congressional requesters, financial regulators are exploring the implementation of technology into the BSA/AML framework such as blockchain analytics and smart contracts to enhance monitoring and enforcement of compliance in the decentralized environment.⁸⁰ However, crypto developers employ agile technology skillsets that are ever beyond regulators' knowledge, making regulator-crypto developers' collaboration more considerable for effective monitoring of activities inside the crypto environment.

Amendment of the BSA/AML regulation to allow incorporation of blockchain analytics will help law enforcers combat illicit activities perpetrated in the crypto environment.⁸¹ Blockchain analytics employs machine learning-based forensics to scrape publicly accessible transactional data and link cryptocurrency holdings to criminal activities.⁸² This process is automatically executed through the help of smart contracts once predetermined conditions are met.⁸³ The blockchain permanently records transactions executed with a crypto wallet, without any possibility of being changed or deleted.⁸⁴ Through the scraping process, blockchain analytics relate crypto transactions to illegal activities through particular signifiers like a crypto wallet previously used for illegal activities.⁸⁵ This follows the identification of a wallet address that is then assigned a "risk score." According to GAO report to Congressional requesters, adequate collaboration between business entities with

⁷⁴ Naja C. Maelle, Chapter 8: Perspectives of a Distributed Future: Aspects of Criminal Law.

⁷⁵ Vishal Gaur (2020). Building a Transparent Supply Chain. *Harvard Business Review*, June.

⁷⁶ Moody's Analytics (2023). Crypto, Compliance, and Customer Due Diligence. April 27.

⁷⁷ Elizabeth Howcroft (2023). Crypto Crime Hits Record \$20 bln in 2022. *Reuters*, January 13.

⁷⁸ Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets* (February 16,).

⁷⁹ US DOJ (2022). Report of the Attorney General's Cyber Digital Task Force. *Cryptocurrency Enforcement Framework*, October.

⁸⁰ See GAO (2023). Blockchain in Finance. Report to Congressional Requesters, June.

⁸¹ *Id.*

⁸² Nadia Pocher, Mirko Zichichi, Fabio Merizzi, Muhammad Zohaib Shafiq and Stefano Ferretti (2023). Detecting Anomalous Cryptocurrency Transactions: An AML/CFT Application of Machine Learning-Based Forensics. *Electron Markets*, 33, 37.

⁸³ *Id.*

⁸⁴ David Rodeck and Micheal Adams (2023). Understanding Blockchain Technology. *Forbes*, May 23.

⁸⁵ *Id.*

providers of blockchain analytics is necessary for screening of crypto transaction to generate a risk score for the wallet address being used.⁸⁶

4.3. Strengthen International Cooperation

Cryptocurrencies operate in a decentralized environment that facilitate seamless cross-border transactions without passing through intermediate proxies such as central authorities.⁸⁷ Based on this global nature of cryptocurrencies, it is challenging to collectively prevent illicit activities executed in the crypto environment due to the varying regulatory requirements from one jurisdiction to the other.⁸⁸ The regulatory arbitrage theory posits that the confusion created by variations in regulatory requirements as deemed appropriate by individual jurisdictions, helps malicious actors to apply financial engineering to restructure their transactions and circumvent unfavorable environments to favorable ones.⁸⁹

The GAO report stresses the need for the BSA/AML to foster international cooperation and coordination to address fraud and money laundering risks perpetrated through seamless transfer of cryptocurrencies between different jurisdictions that use different regulatory standards.⁹⁰ Regulators across the globe need to embrace this call by working together to develop common standards that if incorporated into the BSA/AML framework, might make it enforceable to crypto transactions across different jurisdiction, thus, mitigate against fraud risks executed through cross-border transfers.

5. Conclusion

The study focused on examining the implications of cryptocurrencies on the BSA/AML regulation. Since 1982 when the idea behind cryptocurrency was first mentioned, many people across the world have embraced blockchain technology, ensuring an increased market growth for crypto assets. However, the literature herein, demonstrated how cryptocurrency growth continue to pose risks to the stability of the financial system, raising the need for federal financial regulators to address them and ensure financial stability while maintaining the integrity of the financial system. A challenge that has been established to hinder effective regulation of cryptocurrencies is the absence of a dedicated primary regulator with utmost authority to oversee all activities carried out in the crypto environment. Although the current BSA/AML framework is appropriately comprehensive to cover all the activities carried out in centralized finance to ensure compliance and regulatory goals are achieved, it has not equally been applied to decentralized finance. The previous case proceedings and prosecutions have cited the lack of a physical equivalency of centralized finance to decentralized finance as an obstacle limiting effective prosecution of crimes that require a movable good. Thus, the BSA/AML framework has not optimally provided consistent financial oversight to decentralized finance as it does to centralized finance where it ensures institutions, products, risks, and services are subjected to consistent regulation, oversight, and transparency. Arguably, the federal financial regulators, particularly, SEC and CFTC have been on the forefront of addressing risks related to cryptocurrencies. However, they have still been limited in their current application, creating a gap that has allowed users of crypto assets to enjoy special treatment that has allowed malicious actors to execute their illicit activities anonymously. Efforts to embrace effective adoption and incorporation of crypto assets into the financial system have been made through various legislative histories and Acts such as the CANSEE) Act (S.2355), which targets money laundering, as well as sanction evasion that involves DeFi. Still, the dynamic nature of blockchain technology continues to prove difficult for regulators to adequately understand and control.

6. Recommendations

The study identified gaps in the current BSA/AML framework as it pertains to financial regulations, which need to be addressed for effective and secure adoption of cryptocurrencies into the financial system. Accordingly, this study makes the following two recommendations:

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *Id.*

⁹⁰ *Id.*

The absence of a primary regulator for DeFi proves to be a limiting factor towards effective regulation of cryptocurrencies. Accordingly, this study recommends the enactment of a legislation that will designate a primary regulator with powers to provide a comprehensive regulatory oversight for activities carried out in the crypto environment. The legislation may comprise subsections such as regulatory requirements for operating crypto activities; requirements for participants of DeFi to comply with regular audits and public disclosure of their crypto assets; redemption rights; and minimum requirements for the composition of crypto assets.

Financial regulators have been coordinating venues to address risks posed by cryptocurrencies. However, these efforts have not managed to adequately regulate activities executed in the DeFi environment. Accordingly, this study recommends the Comptroller of the Currency to jointly adapt a formal coordination strategy for financial regulators that include SEC, the Federal Reserve, CFTC, and FDIC for collective identification of risks posed by cryptocurrency related activities and formulate effective regulatory response. This approach may be achieved through formal collection and sharing of information that identifies and records the frequency of crypto activities as they occur in the DeFi environment for effective identification of risks to ensure a timely respond. This coordination will enhance security of consumers and investors, prevent illegal activities, and foster legitimate innovation that would make the U.S economic sector more competitive.

7. Future Areas of Research

Cryptocurrencies seem inevitable to embrace and the only way to be safe, is to find appropriate, effective, and secure approaches for adopting them to mitigate against the risks they pose. Accordingly, it is important that future studies consider investigating the following three blockchain categories.

1. Products and services that are offered in DeFi environment.
2. Trading platforms for cryptocurrencies.
3. Stablecoins.

This is attributed to uncontrollable growth, rampant exposure to retail consumers, and the potential risks that blockchain products and services pose to consumers, investors, and the financial system. A study in these three areas will help advance the knowledge of financial regulators about the loopholes that developers of blockchain technology capitalize on to circumvent unfavorable regulations, and maintain entitlement to special treatment in terms of exemptions from certain regulatory and compliance requirements, contrary to what the centralized finance experience under the same regulatory framework, whereas the two sectors are supposed to compete fairly. Bibliography

References

- Antal-Molnar Nikolett (2022). *The Evolution of the Digital Currency. IJCBE*, 3(1), 1-11.
- Berg Chris, Davidson Sinclair and Potts Jason (2019). *Chapter 8: Public Policy in a Blockchain Era. In Understanding the Blockchain Economy, Monograph Book*, 138-151 (ebook). DOI: <https://doi-org.albanylaw.idm.oclc.org/10.4337/9781788975001.00013>
- Bugár Somogyvári (2020). *Bitcoin: Digital Illusion or a Currency of the Future?. Financial and Economic Review*, 132-153.
- Chaum (1983). *Blind Signature for Untraceable Payments. In Chaum D., Advances in Cryptology*, 199-203.
- Claire Chambers-Jones (2012). *Chapter 5: A Real Crime in a Virtual World. In Virtual Economies and Financial Crime, Monograph Book* (ebook). DOI: <https://doi-org.albanylaw.idm.oclc.org/10.4337/9781849809337.00012>
- Claire Chambers-Jones and Hillman Henry (2014). *Chapter 6: Digital Currencies and Financial Crime. In Financial Crime and Gambling in a Virtual World, Monograph Book*, 137-165 (ebook). DOI: <https://doi-org.albanylaw.idm.oclc.org/10.4337/9781782545200.00012>
- Coie Perkins (2021). *The Anti-Money Laundering Act of 2020: A Survey of Key Provisions and Practice Takeaways. Bloomberg News*, April 13.

- Duggan Wayne and Adams Micheal (2023). *How Does the SEC Regulate Crypto*. *Forbes*, June 30.
- Eberle Edward J. (2011). *The Mythology of Comparative Law*.
- Epstein Lee and Andrew D. Martin (2014). *An Introduction to Empirical Legal Research*.
- Hertig Alyssa (2016). *Ethereum's Two Ethereum Explained*. *CoinDesk*, July 28.
- Hoecke Mark van (2017). *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?*. Bloomsbury Publishing India Pvt. Ltd.
- Huber Sornette (2013). *Boom, Bust, and Bitcoin: Bitcoin-Bubbles as Innovation*. Swiss Finance Institute Research Paper No. 20-41, 1-25.
- Jan Friedrich and Matthias Thiemann (2020). *The Economic, Legal and Social Dimensions of Regulatory Arbitrage*. December 8.
- Katja Langenbucher (2020). *Regulatory Arbitrage: What's Law Got to Do with It?*. July 16.
- Keene Shima (2011). *Emerging Threats: Financial Crime in the Virtual World*. *15 Journal of Money Laundering Control*, 1, 25-37 (ebook). DOI: 10.1108/13685201211194718
- Lemire Katherine A. (2022). *Cryptocurrency and Anti-Money Laundering Enforcement*. *Reuters*, September 26. <https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/>
- Levine Matt (2022). *The Only Crypto Story You Need*. *Bloomberg*, October 25. <https://www.bloomberg.com/features/2022-the-crypto-story/>
- Maelle Nadja C. (2019). *Chapter 8: Perspectives of a Distributed Future: Aspects of Criminal Law*. In *Blockchains, Smart Contracts, Decentralized Autonomous Organizations, and the Law*, Monograph Book, 215-239 (ebook). DOI: <https://doi-org.albanylaw.idm.oclc.org/10.4337/9781788115131.00014>
- Mishra Parikshit (2023). *Infamously Hacked Crypto Exchange Mt. Gox Delays Repayment Deadline by a Year*. *CoinDesk*, September 21. <https://www.coindesk.com/business/2023/09/21/mt-gox-pushes-repayments-by-a-year/>
- Morris David Z. (2023). *How the DAO Hack Changed Ethereum and Crypto*. *CoinDesk*, May 9.
- Nedzel Nadia E. (2004). *Legal Reasoning, Research, and Writing for International Graduate Students*.
- Paris Marie-Luce (2016). *The Comparative Method in Legal Research: The Art of Justifying Choices*.
- Riles Annelise (2014). *Managing Regulatory Arbitrage: A Conflict of Laws Approach*. *Cornell International Law Journal*.
- Shukla Gaurav (2023). *Doctrinal Legal Research: A Library-Based Research*.
- Stevens Rober (2023). *Securities vs. Commodities: Why it Matters in the Crypto Market*. *Coindesk*, May 5.

Websites

- Bogarat Rice (2018). *A Very Brief History of Blockchain Technology Everyone Should Read*. *Forrás*. <https://ripple.com/insights/needham-report-welcome-to-the-internet-of-value/>
- Davitian Law, P.A. (2022). *The Bank Secrecy Act and Cryptocurrency*, *Cryptocurrency Cases*. <https://davitianlaw.com/cryptocurrency-defense/bank-secrecy-act/>
- Global Legal Research Directorate (2021). *Regulation of Cryptocurrency Around the World*. *The Law Library of Congress*. <http://www.law.gov>
- Statista (2023). *Bitcoin (BTC) Price per Day from April 2013-November 16*. <https://www.statista.com/statistics/326707/bitcoin-price-index/>

Cite this article as: Kwabena Akyeampong and Robert Munro (2025). *The Implications of Cryptocurrencies on the US BSA/ AML Regulation*. *International Journal of Cryptocurrency Research*, 5(2), 98-112. doi: 10.51483/IJCCR.5.2.2025.98-112.