ISSN (Print): 2788-8320 ISSN (Online): 2788-8339

JOURNAL OF SOCIAL RESEARCH DEVELOPMENT
www.jsrd.org.pk editor@jsd.org.pk

HARMONIZING INTERNATIONAL LAW FOR DECENTRALIZED AGE: ADDRESSING THE BITCOIN MONEY LAUNDERING THREAT

Kainaat Shah[1], Sardar Yasir Baig[2] & Lubaisha Bint Sohrab[3]

[1]Advocate High Court, Khyber Pakhtunkhwa Bar Council, Khyber Pakhtunkhwa, Pakistan
[2]Student, Business Professional People (BPP) University London, United Kingdom
[3]Lecturer law, Mohi-Ud-Din Islamic University Nerian Sharif, AJK, Pakistan

KEYWORDS

Bitcoin, Money Laundering, Cryptocurrency Regulation, International Legal Framework, Anti-Money Laundering (AML)

ARTICLE HISTORY

Date of Submission: 16-11-2024
Date of Acceptance: 19-12-2024
Date of Publication: 20-12-2024

ABSTRACT

In an abbreviated time, bitcoin and other cryptocurrencies began soaring into a meteoric rise in the world financial market. There is opportunity and, like any growth, some new grave challenges, in the transnational money laundering. The centralization of all this has made it possible for a variety that of money laundering over Bitcoin, especially over Bitcoin, which has operated on the global financial system because it has been decentralized and anonymous. This research proposes the idea of international Bitcoin-enabled harmonized legal framework to combat context of international money laundering. To succeed, however, this framework needs both the private and public sectors working together to resolve tradeoff between privacy and security on the one hand and technological feasibility on the other hand. Both this international approach and collaborative approach will be essential, leading to development of this new industry, including the use of international organizations, national governments as well as the cryptocurrency industry itself. In this linking, the main purpose consists of constructing the rock–solid decentralized infrastructure for the industry, which will rest upon a more reliable and resistant decentralized global financial system.

Correspondence **Kainaat Shah**
Email: shahkainaat13@gmail.com
DOI https://doi.org/10.53664/JSRD/05-04-2024-01-01-16

INTRODUCTION

The rapid growth of Bitcoin and other cryptocurrencies has transformed global financial landscape (Yeung & Galindo, 2019). Decentralized digital currencies have brought new opportunities and significant challenges, especially regarding transnational money laundering (Teichmann & Falker, 2020). Current international legal frameworks prove themselves obscure in tackling this emerging

threat capably because of transnational nature of Bitcoin-enabled money laundering (Leuprecht, Jenkins & Hamilton, 2022). The unique features of Bitcoin, including the decentralization as well as pseudonymity, support the misuse of cryptocurrency for illegal financial activities (Chen, Dong & Li, 2022). However, criminals have exploited these features to hide illegal proceeds of various money laundering typologies, like smurfing, online casinos, mixing/tumbling & initial coin offerings (ICOs) (Teichmann & Falker, 2020; Wu, Lin, Lin, Zheng, Huang & Zheng, 2023). The international antimoney laundering instruments in existence, namely, FATF recommendation and UN Convention against the transnational organized crime, are designed for the centralized and boundary-limited transactions and, thus, fall short in dealing with the decentralized and borderless nature of Bitcoin (Wronka, 2021).

Another problem is that international cooperation is undermined by challenges of international cooperation, such as issues with information sharing, as well as variations in the legal classification of cryptocurrencies within the jurisdictions (Chen, Dong & Li, 2022; Kushnirenko & Kharatishvili, 2023). To effectively combat bitcoin money laundering, international harmonized legal framework that includes the rule of law as well as technological solutions is necessary (Ojih, Joshi, Mohture & Gupta, 2022). Finally, it is concluded that the Bitcoin-enabled money laundering, predicated on its transnational nature, has revealed the shortcomings of existing international legal frameworks in response to developing threat. The need for harmonization of international financial law to combat cryptocurrencies for illegal financial activities is clear: in particular, regulatory and technological tools are to be developed. Within the proposed framework, based on the technological neutrality, proportionality, international cooperation and regulatory clarity principles, an inclusive solution to challenges stemming from Bitcoin's nature as a decentralized, borderless currency is provided. This framework mixes knowledge and cooperation of international organizations, national governments & cryptocurrency market to make possible a safer & coherent planetary financial system in context of decentralized money.

LITERATURE REVIEW

In recent years, Bitcoin and, more generally, cryptocurrencies have fueled seismic shifts in global financial landscape (opportunities & challenges) and transnational money laundering (Stefánsson, Grímsson, Þórðarson & Óskarsdóttir, 2022; Fletcher, Larkin & Corbet, 2021), labeled 'good' moment and a 'bad' moment by President Trump. Bitcoin has been subject to a number of money laundering typologies, can have economic impacts on global financial system as a result of its decentralized and pseudonymous nature (Ferwerda, Deleanu & Unger, 2019; Wegberg, Oerleman & Deventer, 2018). The foundation of this framework should be technological neutrality, proportionality, international cooperation (See, 2023; Nizovtsev, Parfylo, Barabash, Kyrenko & Smetanina, 2021) and regulatory clarity. This framework features the improvement of KYC/AML requirements for cryptocurrency service providers, development of international standards for blockchain analytics and transaction monitoring (Zouhair & Kasraie, 2019; Song, 2023), the creation of a global platform for information and legal cooperation between law enforcement agencies, and harmonization of legal definitions & classifications of cryptocurrencies. Still, some thorny issues of privacy and security, technological feasibility, as well as the scalability must be addressed for this framework to take shape (See, 2023; Gikonyo, 2019).

Bitcoin-related money laundering is genuinely a major issue, as the volume of money laundering is approximately $76 billion annually, as estimated by Leuprecht, Jenkins and Hamilton (2022). The purpose of this research paper is to discover the main principles and elements of such a framework on experience basis and theoretical grounding of several international organizations and research, namely "fraud detection and anti-money laundering applying machine learning techniques in the cryptocurrency transactional graphs", 2023). With industry, national governments & international organizations working together to harmonize this approach, we can deliver a resilient, more secure, globally decentralized financial system (Budiman, 2023; Tomacheski, 2023). While the framework solves immediate problem of Bitcoin as a tool for money laundering, it has greater consequences for destinations of global financial regulation. Still, disruption of decentralized technologies in current financial systems makes it vital to develop flexible, technologically neutral regulatory framework (Gikonyo, 2019; Alshaer et al., 2021). Thus, principles & elements explained in this research should provide guidelines for confronting other emerging digital asset and financial innovation challenges to realize benefits of technology and balance it against associated risks to global financial system (Krištoufek, 2015).

RESEARCH METHODOLOGY

This paper applies a qualitative research methodology that involves performing a thorough review of the academic literature and journal articles. It endeavors to address the problem with Bitcoin-enabled money laundering and requirement for an international harmonized legal framework. This research utilized a quantitative approach because it provides an exploratory technique to gain the deep(er) understanding of complex issues in transnational aspect of cryptocurrency-related money laundering activities (Moss, Donnellan & Neill, 2012; Gorecki, Briggs & Nixon, 2010). This research attempts to understand the basic principles, actors, and practicalities of a harmonized international legal framework that could effectively counter this threat from examining extant body of research. The relevant literature was reviewed via systematic search and analysis of journal articles, research papers, and reports, including law, finance, criminology, and international relations (Frost, Nolas, Gordon, Esin, Holt, Mehdizadeh & Shinebourne, 2010; Gagliardi & Row, 2011). There is a need for a harmonized international legal framework to effectively combat the threat of money laundering via Bitcoin. We carefully evaluated the selected sources on the basis of their methodology quality, depth of the analysis, and content relevance to the research goals (Chisita, 2021; Tanin, Ahmad & Muneeza, 2021).

Aslani and Naaranoja (2015) and Hermansyah (2023) used the qualitative content analysis of the literature to document, identify and explore the key themes, trends and gaps in existing knowledge. The example of cryptocurrencies enabled exploration of how money laundering can be arranged with the help of cryptocurrencies, specifying the specialties of the cryptocurrencies in the money laundering; the shortcomings of modern international legal instruments; and the main principles and attributes, which must be the basis of the development of the common framework (Ban, Baker, Bradley, Elliott, Haskin & Rosengarten, 2021; Bosio & Graffigna, 2012). Moreover, it helps analyze challenges and implementation considerations in terms of privacy, security, as well as technological feasibility and encourages public–private partnerships (Janssens, Zadelhoff, Loo, Widdershoven &

Molewijk, 2014; Mudhai, 2011). In this linking, the broad recommendations regarding measures to counter the threat of the Bitcoin-enabled money laundering have been formulated via this broad qualitative approach (Johnson, 2014). To facilitate conversation among policymakers, regulators and the cryptocurrency industry on effective means of combating the misuse of cryptocurrencies to finance illicit activity, this research employs a qualitative approach (Lee, Cheng & Zeleke, 2014; Uzuner, 2015).

RESULTS OF STUDY

The explosive rise of Bitcoin and other cryptocurrencies has completely transformed the way world thinks about and does finance. However, this demand presents new opportunities and repercussions for transnational money laundering (Stefánsson et al., 2022; Fletcher et al., 2021). As Bitcoin lacks centralization, pseudonymity, criminals have utilized and exploited a variety of money laundering typologies anonymously, with a considerable impact on the global financial system (Ferwerda et al., 2019; Wegberg et al., 2018). An international, harmonized legal approach should address the threat of Bitcoin to money laundering. This framework express technological neutrality, proportionality, international cooperation and clarity in the regulation principles (Nizovtsev et al., 2021; See, 2023). This framework contains the following elements: cryptocurrency service providers will be required to enhance KYC/AML in accordance with the international standards; to induce the creation of the blockchain analytics and transaction monitoring standards among countries; to establish a global platform for exchange of information and facilitation of work between law enforcement agencies; and to harmonize the legal definitions and classes for the cryptocurrencies (Song, 2023; Zouhair & Kasraie, 2019).

This framework balances privacy and security, technological feasibility and scalability, and strong public-private partnerships (See, 2023; Gikonyo, 2019) for the successful implementation. Through cooperation among international organizations, national governments and cryptocurrency industry, a common way to secure a decentralized financial system on the global scale can be thus achieved (Budiman, 2023; Tomacheski, 2023). The proposed framework not only addresses the immediate threat of Bitcoin-enabled money laundering but can also be applied to global financial regulation in the future. However, decentralized technologies have continued disrupting traditional financial systems and have a strong need for adaptable and technologically neutral regulatory frameworks including law, finance, criminology, and the international relations (Gikonyo, 2019; Alshaer et al., 2021). It outlines principles and elements that can serve as a blueprint for addressing the challenges introduced by other nascent digital assets and financial innovations to allow these innovations to deliver their benefits while achieving risk mitigation for the stability of the global financial system (Krištoufek, 2015).

Bitcoin & Transnational Money Laundering Challenge

Bitcoin's Characteristics that Facilitate Money Laundering

Owing to Bitcoin's decentralized and pseudonymous nature, Bitcoin has become an ideal platform for money launderers trying to illicitly profit from cryptocurrency (Leuprecht et al., 2022; Fletcher et al., 2021). Nevertheless, these features present major obstacles to cross-border investigations and

enforcement actions & facilitate many kinds of money laundering across borders. Decentralization: In Bitcoin network, the lack of central authority makes cross border investigation and enforcement difficult (Fletcher et al., 2021). This is because law enforcement units have no crucial point of control to monitor and track illicit transactions and antireach other jurisdictions to coordinate their efforts (Leuprecht et al., 2022). They can smoothly transfer money across borders that is untraceable and untraceable by criminals. (Fletcher et al., 2021) Pseudonymity: Bitcoin transactions are anonymous, people are anonymous; it is just a wallet address, and it is hard to identify anyone and trace money flows between jurisdictions (Dupuis & Gleason, 2020). The anonymity of source of illicit proceeds and, therefore, of the proceeds themselves to money legally earned (Leuprecht et al., 2022) are also given to criminals.

Speed and low cost of cross-border transactions: Bitcoin transactions are completed in minutes, often with lower fees, making them a viable choice for those seeking to laund money (Fletcher et al., 2021). These transactions are extremely rapid and inexpensive and thus allow for rapid movement of funds across borders, making it harder for law enforcement agencies to detect and break up the incidences of money laundering (Leuprecht et al., 2022). "For example, estimates are that Bitcoin related money laundering abroad is over $76 billion a year (Sultan et al., 2023) and the problem is massive in scale and impact." The ramifications of this illicit activity are far broader, as it jeopardizes the integrity of worldwide financial framework and helps advance criminal activities, including delivery of drugs, terrorism and corruption (2022; 2023). Cryptocurrencies have made transactions, overall, pseudonymous with quick and low cost across borders and diverse Bitcoin to exploit the transnational nature of cryptocurrency to accommodate in minds of money launderers (Leuprecht et al., 2022; Fletcher et al., 2021). To overcome this, we need a full and harmonized international legal framework capable of effectively combating the misuse of cryptocurrencies to finance illegal financial activities.

Money Laundering Typologies Using Bitcoin

Cryptocurrencies have come to fore as tools for facilitating criminal behavior. Owing to Bitcoin's decentralized and pseudonymous nature, various money laundering typologies can be exploited, many have substantial transnational dimension. These methods are fully explored: smurfing, online casinos, mixing and initial coin offerings (Leuprecht et al., 2022). Smurfing: Ease of opening multiple Bitcoin wallets eased smurfing, breaking up of large sums of illicit funds in small sums, bypassing detection. As these wallets make it easy to swap cash fast and, in anonymity, transferring money amid them makes it difficult for law enforcement to trace funds' origin (Dupuis & Gleason, 2020). The online cryptocurrency casinos are evolving into new money laundering vehicles because they allow criminals to defer and potentially integrate illicit proceeds into legitimate financial system by pretending that funds were gambling winnings. Cryptocurrency tumbling or mixing services are heavily abused for money laundering to obfuscate funds' origins by mashing transactions (Budiman, 2023). The services are often conducted across the borders into multiple jurisdictions, making tracing flow of illicit funds challenging. They invest their illicit proceeds into ICOs precisely as they can then infuse these funds into the cryptocurrency ecosystem and eventually take them out as legitimate investments.

Scale & Impact of Problem

Bitcoin money laundering is significant in magnitude and damage, and its amount of occurrence is estimated at more than $76 billion annually worldwide (Foley et al., 2019). This figure is the same as the aggregate size of the U.S. and European illegal drug markets (Foley et al., 2019; Leuprecht et al., 2022). Leuprecht et al. (2022) reported that 46% of all Bitcoin transactions are related to illegal activities, such as money laundering (Foley et al., 2019), which is equivalent to approximately 37 million Bitcoin transactions each year on behalf of criminals. One reason that cryptocurrencies are becoming a prime target for money laundering is because of the deregulated and stateless qualities of cryptocurrencies, allow criminals to conduct global-scale transactions (Leuprecht et al., 2022; Leuprecht et al., 2022). Besides, the cryptocurrency transactions are anonymous and fast, allowing funds to be acquired to fund actual harm to people and communities through the perpetuation of drug trafficking and human exploitation (Foley et al., 2019). The threat of bitcoin money laundering is serious: coordinated and harmonized international legal standpoint is urgently needed (estimated to consist of tens of billions per year) (Foley et al., 2019). We must solve this problem, or financial integrity will continue to deteriorate, and transnational criminal enterprises will spread (Leuprecht et al., 2022).

Inadequacy of Existing ILF

Existing International AML Instruments & their Limitations

Finally, Financial Action Task Force (FATF), an intergovernmental organization established in 1989, has promoted the global effort to combat money laundering (Urooj, 2023). They have established 40 recommendations for the international standard for AML and CFT measures as standardized by the FATF (Urooj, 2023). FATF recommendations have been widely adopted by countries, but they are not applicable to specific issues created by cryptocurrencies, such as Bitcoin (Al-Tawil, 2022). Being decentralized and borderless, digital assets are outside the traditional financial system to which the FATF recommendations were targeted. However, these instruments were created before cryptocurrencies existed and were not designed with tools needed to address these overly concerns of this technology (Rose, 2022). Nevertheless, the cryptocurrency nature of being decentralized and pseudonymous permits law enforcement agencies to work hard to trace and seize illegal funds to be effective (Al-Tawil, 2022). In addition, the diverging legal characterizations of cryptocurrencies from one jurisdiction to another as property, as financial instruments, have led to a domino effect of regulatory patchwork, hampering cross-border cooperation and enforcement. The result of this fragmentation of global regulatory landscape has been a fusion for criminals to exploit these gaps and loopholes, thus exacerbating the challenge of combating bitcoin endemic money laundering (Al-Tawil, 2022).

Challenges to International Cooperation

Cryptocurrencies such as Bitcoin are good mechanisms for laundering money, as they allow the anonymity of their users, the transmitter, the receiver and amount of money involved in transaction, which is characteristic of the decentralized and borderless nature that cryptocurrencies enjoy (Silva & Silva, 2022). According to Silva and Silva (2022), cross-border investigations and enforcement are hampered by the requirement for a centralized authority and the pseudonymous nature of these

digital assets. Because cryptocurrencies are not governed under a single global framework (Tuya et al., 2017), class of cryptocurrencies has been diffused, whereby countries are free to choose whether to categorize cryptocurrencies and manage them or not. Regulatory patchwork has raised barriers to efficient sharing of information and coordination of enforcement actions among law enforcement agencies that have jurisdiction in diverse areas (Yasaka, 2017). Second, there have been diverse classifications of cryptocurrencies, like property and financial instruments, which hinder countries from dealing with issue of cooperation in investigating or prosecuting cryptocurrencies. However, owing to the lack of harmonization, there are gaps in the loopholes of the global regulatory system that criminals have used to impede operational efforts to facilitate the international cooperation (Kamau et al., 2021).

Role of National Laws & Regulations

The successful development of cooperation at the international level to eliminate the vulnerability of Bitcoin to be used in process of money laundering was influenced by diverse national approaches in the regulation of cryptocurrencies (Artemov et al. 2020; Dhali et al., 2023). The approaches of countries around the world have drastically differed in how they have understood, regulated, and legislated the usage of cryptocurrencies (Arindrajaya & Koos, 2022; Sham et al., 2023). Owing to this shortcoming of the harmonization, criminals can, among others, operate their criminal networks across jurisdictions where criminality is weakly regulated & (almost) never detected or prosecuted (Dhali et al., 2023; Putri, 2023). In this linking, with some countries such as the United States and Canada, cryptocurrencies, like all other assets, have been treated as taxable assets (Al-Tawil, 2022; Bartoletti et al., 2021). However, Indonesia takes a different position. According to Putri (2023) and Teichmann and Falker (2020), the diverse legal classifications of lovebirds have prevented support at the cross-border level, as confined law enforcement agencies lack the ability to coordinate and communicate with each other to attain desired outcomes. However, clear and consistent regulations are lacking, which has resulted in uncertainty within businesses and consumers at both ends of the trade, undermining the integrity of the global financial system (Auer & Lucas, 2022; Lucchini et al., 2020).

Toward a Harmonized ILF

Principles for a New Framework

However, to effectively combat the threat of Bitcoin-enabled money laundering, an international legal framework needs to be developed on basis of set of guiding principles adapted to the specific challenges these cryptocurrencies offer (Teichmann & Falker, 2020; Feinstein & Werbach, 2021). Principle of Technological Neutrality: Instead of focusing on Bitcoin, regulations should focus on activity (money laundering) (Battalova et al., 2019; "Comparative and informative characteristic of the legal regulation of blockchain and cryptocurrency: state and prospects," 2021). This principle of technological neutrality ensures adaptability to constantly changing reality of cryptocurrencies and other types of emerging digital assets (Dumchikov et al., 2020; Silva & Silva, 2022). Principle of proportionality: AML measures should be balanced to risks such cryptocurrency activities pose (Monsalve et al., 2020; Avşar & Serin, 2021). This principle recognizes that not all cryptocurrency uses cases carry the same level of money laundering risk and that the regulatory response should be

tailored accordingly (Tsindeliani, 2020; "Cryptocurrency Acceptance: A Case of Malaysia," 2019). Thus, to combat the transnational nature of Bitcoin-based money laundering (Teichmann & Falker, 2020; Su et al., 2023), information sharing and codesirable enforcement actions among countries are important.

Key Elements of a Harmonized Framework

A practical, robust international legal framework to fight against Bitcoin money laundering will have to combine set of improved regulatory measures, technological enhancements and reinforced international cooperation. Several key elements are vital for success of such a framework: Enhanced KYC/AML Requirements for Cryptocurrency Service Providers Globally: Effective AML regime is, in effect, incomplete, lacking robust Know Your Customer (KYC) & Anti-Money Laundering (AML) requirements. In fact, while, level of KYC and AML compliance differs across cryptocurrency service providers, some of them are run in jurisdictions with no or exceptionally light regulations. However, harmonized framework must insist on the stringent KYC/AML requirements for all cryptocurrency service providers worldwide, regardless of their residence. It includes cryptocurrency exchanges, custodians, wallet providers and others that facilitate the transfer or exchange of cryptocurrencies. Customer due diligence, transaction monitoring, suspicious activity reporting, and recordkeeping obligations be component requirements under these matters. As such, standardized procedures and protocols should be developed for these procedures to ensure consistency and effectiveness across jurisdictions. The enforcement of these requirements entails the international cooperation so that the regulatory arbitrage (business move to jurisdictions with the weaker regulations) will not occur (Orlovskyi, 2023).

Role of International Organizations

The development and implementation of a harmonized legal framework to fight the Bitcoin money laundering relies on international organizations. Thus, several organizations are particularly well positioned to contribute to this effort: The Financial Action Task Force (FATF): Since its inception, the FATF has been the global standard setter for AML/CFT and now has a crucial mandate to adapt its recommendations to address the challenge cryptocurrencies pose to the AML/CFT regime. This process has already started by the FATF with the issue of guidance on virtual assets and virtual asset service providers. However, more needs to be done to implement & enforce FATF recommendations globally, much more. In this connection, much like normal, however, the FATF should still account for emerging developments in the cryptocurrency field as well as modify its guidance, if necessary, legislated the usage of cryptocurrencies in the diverse circumstances (Rose, 2020; Guo, 2023). The United Nations (UN): Through a number of agencies and conventions, however, the UN can create a comprehensive international legal framework that have jurisdiction in diverse areas. For example, there is the basis for international cooperation in combatting money laundering vested in the UN Convention against the Transnational Organized Crime. In addition, the UN can sponsor capacity-building programs for law-enforcing agencies in developing countries (Umar, 2023; Alarab and Prakoonwit, 2022).

Addressing Challenges & Implementation Considerations

Balancing Privacy & Security

The regulation of cryptocurrencies presents a central tension between AML requirements on one hand and individual privacy rights on the other. As vital in fight against money laundering, these enhanced know your customer and measures against money laundering must inevitably include data collection and data sharing. Then, there is the ability for this to be abused and the eroding of privacy. Finding the right balance is crucial, which may enable AML regulations to protect public trust but not with respect to fundamental rights Koutsoupia (2023). Regarding this tension, there is path to explore potential of privacy-enhancing technologies. Zero knowledge proof, homomorphic encryption, and secure multiparty computation are technologies that create methods in which information can be verified without revealing the underlying data (Makarov & Schoar, 2022). For example, user could verify that they are over certain age or fulfill other KYC requirements without revealing their extremely specific birth date or other personal information. Similarly, transactions can also potentially be analyzed for indications of suspicious patterns without disclosing the parties' identities or amounts being transferred. Bringing PETs into AML/KYC procedures could improve regulatory compliance and guarantee user privacy. Still, some technical challenges exist for PETs, as do some limitations & vulnerabilities that need to be considered on their implementation (Paesano & Siron, 2022).

Technological Feasibility & Scalability

The evolution of the regulatory framework is challenged by the rapid evolution of cryptocurrency technology. The new cryptocurrencies, blockchain platforms, and privacy-enhancing technologies always emerge, and while industry is dynamic and growing, these technologies are also complex. These changes create almost impossible task for regulations, which must be technologically neutral and adaptable to keep up with these changes & not be quickly made obsolete (Böhme et al., 2015). Another vital point is scalability. Though designed to be transparent, Bitcoin blockchain becomes a bottleneck at some point when transaction grow. The computational challenge lies in analyzing and monitoring millions of transactions in real time. Some of these pressures could be alleviated by solutions such as off-chain transactions and Layer 2 scaling. However, integration of these solutions into AML/KYC workflows is delicate enough to plan and manage (Huang et al., 2022). In addition, because privacy coins provide extra anonymity, blockchain analytics and transaction monitoring struggle to track these transactions and, even more so, investigate suspicious behavior related to the use of these privacy coins. The challenge for privacy coin needs the development of powerful tools and techniques to cope with privacy coin challenge to maintain the integrity of the AML system (Crettez et al., 2015).

Role of Public–Private Partnerships

To effectively implement proposed framework, strong collaboration between diverse stakeholders, that is, governments, regulators, and the cryptocurrency industry, must be put in place. Technical expertise and innovations for practical solutions sit with industry, but governments and regulators provide legal frameworks and enforcement mechanisms. Collaborative cooperation with the crypto industry in the fight against money laundering has the potential to be achieved in public–private partnerships (Zapivakhin et al., 2018). This collaboration is based on information sharing. The first line of defense for cryptocurrency exchanges & other service providers is usually money laundering.

However, they possess valuable transaction data and can function as key human interfaces for good & bad detection of suspicious activity. The information flow between industry and law enforcement must be clearly established. In combination, such training programs and educational resources can further improve the AML/KYC compliance of the industry as a whole. In addition, the regulatory sandboxes and pilot programs give the companies a sandbox to evaluate out and fine-tune modern technologies and how regulators themselves will approach the modern technologies (Makarov & Schoar, 2022).

DISCUSSION

Bitcoin and other cryptocurrencies have grown exponentially in use around the world, opening new financial avenues yet presenting new currencies of opportunity for global money laundering (Stefánsson et al., 2022; Fletcher et al., 2021). As Bitcoin is devolved and pseudonymous, criminals have been using different money laundering typologies, which pose a significant burden on global financial system, to other extents (Ferwerda et al., 2019; Wegberg et al., 2018). Effective fighting of the threat of money laundering through Bitcoin requires a harmonized international legal regime. The framework be developed on basis of technological neutrality, proportionality, international cooperation and regulatory clarity (See, 2023; Nizovtsev et al., 2021). Elements of this framework, which framework also recognizes, are enhanced KYC/AML requirements, design of international standards for blockchain analytics and transaction monitoring, a global standard platform for law enforcement agencies' information sharing and cooperation, and harmonization of legal definitions and classification of cryptocurrencies (Zouhair & Kasraie, 2019). He argues that this framework has answer to challenge of striking the balance amid privacy and security, technological feasibility, scalability, and need to create environment conducive for public–private partnerships (See, 2023; Gikonyo, 2019).

The harmonized path to making the global financial system more certain and durational in the decentralized age (Budiman, 2023; Tomacheski, 2023) could involve leveraging knowledge and international collaboration of international organizations, national governments & cryptocurrency industry. This research paper proposes a framework for how global regulation might look about in the future in the hope of resolving the current Bitcoin threat of allowing money laundering and, in general, how global financial regulation could evolve into the future (Gikonyo, 2019; Alshaer et al., 2021). While it speaks to a specific asset, this research also highlights principles and components that can serve as a blueprint for handling the issues that other emerging digital assets and financial innovations face so that the benefits of these technologies can be enjoyed, and safeguards can be established to protect the integrity of global financial system (Krištoufek, 2015). This qualitative research study employed a review of scholarly literature and journal articles to address problem of Bitcoin-enabled money laundering & need for a harmonized international legal framework (Moss et al., 2012; Gorecki, et al., 2010). Existing research has analyzed and identified recurring themes, emerging trends, and critical gaps in current knowledge of this topic (Frost et al., 2010; Gagliardi & I row, 2011).

This approach has the advantages of being able to offer subtle analysis of singular cryptocurrency features that enable money laundering, the paucity of existing international legal instruments, and

the main principles and elements required for a harmonized framework (Chisita, 2021; Tanin et al., 2021). Another key element of literature review was an analysis of challenges and implementation considerations in achieving balancing privacy and security and technological feasibility (Aslani & Naaranoja, 2015; Hermansyah, 2023). This comprehensive qualitative approach allows for the creation of balanced evidence based on recommendations to alleviate Bitcoin money laundering threat in tokenized era (Ban et al., 2021; Bosio & Graffigna, 2012). This article calls for international legal harmonization regarding the specific properties inherent in virtual currencies and broader implications for the future of global financial regulation in the decentralized era (Lentsck et al., 2019; Johnson, 2014). This research shows how Bitcoin money laundering is an imminent threat that demands the international harmonization of potential legal agreements to combat this threat. By following these key principles and elements of this study, policymakers and regulators can build an ecosystem of cryptocurrency, which is more secure and transparent, and a global financial system will be prepared to embrace the opportunities and challenges of decentralized age (Lee et al., 2014; Uzuner, 2015).

CONCLUSION

As such, this research has studied intricate challenges presented by Bitcoin to international anti-money laundering. As Bitcoin transactions are decentralized, pseudonymous, and rapidly cross-border, they offer many opportunities for money laundering, and the relevant international legal framework is not suitable for such operations. A review of existing AML regimes naked significant voids at both the international level, in the case of legal tools and practice, regarding information sharing, regulatory harmonization, and the application of 'old style' AML concepts to decentralized currency environment. Significant findings reveal necessity for international legal harmonization on basis of national acts suitable for Bitcoin and similar cryptocurrencies with specific properties. The necessity of this framework lies in the establishment of international standards in the way of blockchain analytics and transaction monitoring for cryptocurrency service providers globally to build secure global platform for information sharing & intelligence cooperation of law enforcement agencies of other countries and the implementation of substantial KYC/AML requirements globally. First, regulatory clarity and practical cross-border cooperation require a unified legal definition and classification of cryptocurrencies. Privacy-enhancing technologies present promising approach to strike appropriate balance between requisite strong AML controls and safeguarding individuals' privacy rights.

Recommendations

1. An international legal framework that is technologically neutral, clear, and proportional and built on principles of international cooperation should be advanced. We should be able to adjust this framework to evolving landscape of cryptocurrencies and other emerging digital assets quickly.
2. All global cryptocurrency service suppliers are required to comply with stringent know your customer & antimoney laundering standards for their services. Development of international standards for blockchain analytics and transaction monitoring, including standard data formats, best practices, and protocols for the cross-border sharing of data, should be promoted to increase investigation capability and enforcement.

3. A safe global channel for accurate time information exchange and collaboration among law enforcement agencies should be created, & definite procedures for providing and requesting assistance in cases of cross-border cases should be defined.
4. To achieve clarity for THE businesses, consumers, and regulators in defining and classifying cryptocurrencies across jurisdiction, they should harmonize legal definitions & classifications of cryptocurrencies and simplify AML regulations and their application.
5. The public–private partnerships can be chosen to maximize the cryptocurrency industry's knowledge and ability to devise workable solutions while conducting rigorous regulation and oversight.

REFERENCES

Alarab, I., & Prakoonwit, S. (2022). Graph-based LSTM for anti-money laundering: experimenting temporal graph convolutional network with bitcoin data. *Neural Processing Letters*, 55(1), 689-707.

Alshaer, H., Said, M., & Rajamanickam, R. (2021). The role of the Palestine monetary authority in combating money laundering. *Journal of Money Laundering Control*, 24(4), 762-774.

Al-Tawil, T. (2022). The Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control*, 26(6), 1150-1164.

Arindrajaya, S., & Koos, S. (2022). Legal protection against cryptocurrency investors: overview of Indonesian consumer protection law. *Journal of Human Rights Culture and Legal System*, 2(2), 113-120.

Artemov, N., Арзуманова, Л., Sitnik, A., Smirnikova, J., & Zenin, S. (2020). The legal regulatory model of virtual currency circulation: a sociolegal study. *Jurídicas Cuc*, 16(1).

Aslani, A., & Naaranoja, M. (2015). Systematic-qualitative research for diffusion of innovation in the primary healthcare centers. *Journal of Modeling in Management*, 10(1), 105-117.

Auer, R., & Tercero-Lucas, D. (2022). Distrust or speculation? the socioeconomic drivers of U.S. cryptocurrency investments. *Journal of Financial Stability*, 62, 101066.

Avşar, İ., & Serin, Z. (2021). Bibliometric analysis of scientific production on international trade and cryptocurrency. *International Journal of Advanced and Applied Sciences*, 8(8), 42-51.

Ban, S., Baker, K., Bradley, G., Derbyshire, J., Elliott, C., Haskin, M., & Rosengarten, L. (2021). 'Hello, my name is ...': an exploratory case study of interprofessional student experiences in practice. *British Journal of Nursing*, 30(13), 802-810.

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: analysis and perspectives. *Ieee Access*, 9, 148353-148373.

Battalova, L., Enikeev, R., Kokanov, N., Semivelichenko, E., & Probichev, V. (2019). Legal regulation of virtual currency: international experience and development trend in Russia. *Humanities & Social Sciences Reviews*, 7(4), 911-914.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). The Bitcoin: economics, technology, and governance. *Journal of Economic Perspectives*, 29(2), 213-238.

Bosio, A., & Graffigna, G. (2012). 'Issue-based research' and 'process methodology': reflections on a postgraduate master's programs in qualitative methods. *Psychology Learning & Teaching*, 11(1), 52-59.

Budiman, A. (2023). Content analysis of legal protection regulations for money laundering victims in Indonesia. *International Journal of Scientific Research and Management*, 11(12), 419-427.

Chen, Q., Dong, S., & Li, J. (2022). Outlook of digital currencies and future restrictions on cryptocurrencies. https://doi.org/10.2991/aebmr.k.220307.130

Chisita, C. (2021). Massive open online courses (moocs): a tool for intercontinental collaboration in archives and records management education in eSwatini. *Records Management Journal*, 31(2), 158-175.

Crettez, B., Deffains, B., & Musy, O. (2015). Convergence of legal rules: comparing cooperative and noncooperative processes. *Review of Law & Economics*, 12(1), 13-35.

Dhali, M., Hassan, S., Mehar, S., Shahzad, K., & Zaman, F. (2023). Cryptocurrency in the darknet: sustainability of the current national legislation. *International Journal of Law and Management*, 65(3), 261-282.

Dumchikov, M., Kononenko, N., Batsenko, L., Halenin, R., & Hlushchenko, N. (2020). Issues of regulating cryptocurrency and control over its turnover: international experience. *Revista Amazonia Investiga*, 9(31), 10-20.

Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, 28(1), 60-74.

Feinstein, B., & Werbach, K. (2021). The impact of cryptocurrency regulation on trading markets. *Journal of Financial Regulation*, 7(1), 48-99.

Ferwerda, J., Deleanu, I., & Unger, B. (2019). Strategies to avoid blacklisting: the case of statistics on money laundering. *Plos One*, 14(6), e0218532.

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: a case for bitcoin regulation. *Research in International Business and Finance*, 56, 101387.

Foley, S., Karlsen, J., & Putniņš, T. (2019). Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies? *Review of Financial Studies*, 32(5), 1798-1853.

Frost, N., Nolas, S., Brooks-Gordon, B., Esin, C., Holt, A., Mehdizadeh, L., & Shinebourne, P. (2010). Pluralism in qualitative research: impact of different researchers and qualitative approaches on the analysis of qualitative data. *Qualitative Research*, 10(4), 441-460.

Gagliardi, A. and Dobrow, M. (2011). Paucity of qualitative research in general medical and health services and policy research journals: analysis of publication rates. *BMC Health Services Research*, 11(1).

Gikonyo, C. (2019). The legal profession in kenya and its anti-money laundering obligations or lack thereof. *Journal of Money Laundering Control*, 22(2), 247-256.

Gorecki, C., Briggs, M., & Nixon, J. (2010). Evaluation of five search strategies in retrieving qualitative patient-reported electronic data on the impact of pressure ulcers on quality of life. *Journal of Advanced Nursing*, 66(3), 645-652.

Guo, C. (2023). Lb-glat: long-term bigraph layer attention convolutional network for anti-money laundering in transactional blockchain. *Mathematics*, 11(18), 3927.

Hermansyah, S. (2023). Investigating difficulties faced by lecturers in teaching general english. *Journal of English Education and Teaching*, 7(3), 499-509.

Huang, T., Lee, N., & Chen, W. (2022). Dilemmatic dual-factor determinants of discontinuous intention in cryptocurrency usage. *Information Technology and People*, 36(2), 564-594.

Janssens, R., Zadelhoff, E., Loo, G., Widdershoven, G., & Molewijk, B. (2014). Evaluation and perceived results of moral case deliberation. *Nursing Ethics*, 22(8), 870–880.

Johnson, J. (2014). 'Studying up': researcher as supplicant in feminist studies of elite spaces of work. *International Journal of Gender & Women Studies*, 2(3), 01–12.

Kamau, L., Mwangi, W., & Mwaeke, P. (2021). Examination of barriers of criminal information sharing between law enforcement agencies and their effect in crimes management in nairobi county, Kenya. *European Journal of Humanities and Social Sciences*, 1(5), 11–17.

Koutsoupia, V. (2023). Challenges of the use of virtual assets in money laundering. *Nordic Journal of European Law*, 6(4), 53–78.

Krištoufek, L. (2015). What are the main drivers of the bitcoin price? evidence from wavelet coherence analysis. *Plos One*, 10(4), e0123923.

Kushnirenko, S., & Kharatishvili, A. (2023). Cryptocurrencies turnover and forensic analysis of the mechanism of committing crimes. *Kutafin Law Review*, 9(4), 774–792.

Lee, C., Cheng, C., & Zeleke, A. (2014). Can text mining technique be used as an alternative tool for qualitative research in education? 1–6. https://doi.org/10.1109/snpd.2014.6888691

Lentsck, M., Marcon, S., & Baratieri, T. (2019). Uso do estudo de caso qualitativo pela enfermagem brasileira: uma revisão integrativa. *Revista Enfermagem Atual in Derme*, 84(22).

Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, 30(4), 1036–1054.

Lucchini, L., Alessandretti, L., Lepri, B., & Baronchelli, A. (2020). From code to market: network of developers and correlated returns of cryptocurrencies. *Science Advances*, 6(51).

Makarov, I., & Schoar, A. (2022). Cryptocurrencies and decentralized finance (defi). https://doi.org/10.3386/w30006.

Monsalve, S., Suárez-Cetrulo, A., Cervantes, A., & Quintana, D. (2020). Convolution on neural networks for high-frequency trend prediction of cryptocurrency exchange rates using technical indicators. *Expert Systems with Applications*, 149, 113250.

Moss, H., Donnellan, C., & O'Neill, D. (2012). A review of qualitative methodologies used to explore patient perceptions of arts and healthcare. *Medical Humanities*, 38(2), 106–109.

Mudhai, O. (2011). Immediacy and openness in a digital Africa: networked-convergent journalisms in Kenya. *Journalism*, 12(6), 674–691.

Nizovtsev, Y., Parfylo, O., Barabash, O., Kyrenko, S., & Smetanina, N. (2021). Mechanisms of money laundering obtained from cybercrime: legal aspect. *Journal of Money Laundering Control*, 25(2), 297–305.

Ojih, J., Joshi, P., Mohture, A., & Gupta, S. (2022). Crypto-hesitancy: is regulation the answer? *Journal of Indian Business Research*, 15(1), 9–22.

Orlovskyi, R. (2023). Legalization of criminally obtained property committed by organized criminal groups: european and ukrainian standards. *Jurídicas Cuc*, 19(1).

Paesano, F. and Siron, D. (2022). Working paper 38: cryptocurrencies in asia and beyond: law, regulation and enforcement. *Basel Institute on Governance Working Papers*, (38), 1–69.

Putri, T. (2023). Inadequate cryptocurrency and money laundering regulations in indonesia (comparative law of us and germany). *Yustisia Jurnal Hukum*, 12(2), 129.

Rose, C. (2022). Enforcing the 'community interest' in combating transnational crimes: the potential for public interest litigation. *Netherlands International Law Review*, 69(1), 57–82.

Rose, K. (2020). Disclosing anti-money launderers through csr regulation – a new way to combat money laundering. *Journal of Money Laundering Control*, 23(1), 11–25.

See, K. (2023). The satoshi laundromat: a review on the money laundering open door of bitcoin mixers. *Journal of Financial Crime*, 31(2), 416–426.

Sham, R., Aw, E., Abdamia, N., & Chuah, S. (2023). Cryptocurrencies have arrived, but are we ready? unveiling cryptocurrency adoption recipes through a SEM-FSQCA approach. *The Bottom-Line Managing Library Finances*, 36(2), 209–233.

Silva, E., & Silva, M. (2022). Research contributions and challenges in dlt-based cryptocurrency regulation: a systematic mapping study. *Journal of Banking and Financial Technology*, 6(1), 63–82.

Song, J. (2023). Hbtbd: a heterogeneous bitcoin transaction behavior dataset for the anti-money laundering. Applied Sciences, 13(15), 8766.

Stefánsson, H., Grímsson, H., Þórðarson, J., & Óskarsdóttir, M. (2022). Detecting potential money laundering addresses in bitcoin blockchain using unsupervised machine learning. https://doi.org/10.24251/hicss.2022.194.

Su, C., Song, Y., Chang, H., Zhang, W., & Qin, M. (2023). Could cryptocurrency policy uncertainty facilitate u.s. carbon neutrality? *Sustainability*, 15(9), 7479.

Sultan, N., Mohamed, N., Martin, M., & Latif, H. (2023). Virtual currencies and money laundering: existing and prospects for jurisdictions that comprehensively prohibited virtual currencies like Pakistan. *Journal of Money Laundering Control*, 27(2), 395–412.

Tanin, T., Ahmad, A., & Muneeza, A. (2021). Shariah-compliant equities and shariah screening: need for convergence of ethical screening of stocks with shariah screening. *International Journal of Emerging Markets*, 18(2), 296–315.

Teichmann, F. and Falker, M. (2020). Cryptocurrencies and financial crime: solutions from liechtenstein. *Journal of Money Laundering Control*, 24(4), 775–788.

Tomacheski, C. (2023). The nilcatenation problem and its application for detecting money laundering activities in cryptocurrency networks. *International Transactions in Operational Research*, 31(6), 3955–3974.

Tsindeliani, I. (2020). Cryptocurrency: problematic aspects of legal regulation. *Annual Center Review*, (12–13), 15–21.

Tuya, M., Cook, M., Sutherland, M., & Luna-Reyes, L. (2017). Information requirements to create public value: sharing and opening data to address urban blight. *Transforming Government People Process and Policy*, 11(1), 79–98.

Umar, B. (2023). Is combatting money laundering an integrity issue? insights from Nigeria. *Journal of Money Laundering Control*, 27(4), 687–695.

Urooj, S. (2023). A dynamic threshold analysis of effect of financial action task force (FATF) measures on financial inclusion: evidence from the world. *Journal of Money Laundering Control*, 27(4), 696–709.

Uzuner, Y. (2015). A critical examination of my qualitative research efforts in turkey. *Journal of Qualitative Research in Education*, 3(3), 44–54.

Wegberg, R., Oerlemans, J., & Deventer, O. (2018). Bitcoin money laundering: mixed results? an explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 00-00.

Wronka, C. (2021). Anti-money laundering regimes: a comparison between germany, switzerland and the uk with a focus on the crypto business. *Journal of Money Laundering Control*, 25(3), 656-670.

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). The Financial crimes in web3-empowered metaverse: taxonomy, countermeasures, and opportunities. *Ieee Open Journal of the Computer Society*, 4, 37-49.

Yasaka, N. (2017). Data mining in anti-money laundering field. *Journal of Money Laundering Control*, 20(3), 301-310.

Yeung, K. and Galindo, D. (2019). Why do public blockchains need formal and effective internal governance mechanisms? *European Journal of Risk Regulation*, 10(2), 359-375.

Zapivakhin, I., Ilin, I., & Levina, A. (2018). Public private partnership as city project management technology. *Matec Web of Conferences*, 170, 01037.

Zouhair, A. and Kasraie, N. (2019). Disrupting fintech: key factors for adopting bitcoin. *Business and Economic Research*, 9(2), 33.