On Cryptocurrencies: Guidelines for a Global Legal Framework to Mitigate Insolvency Risks

Lauren Rice[*]

DOI: https://doi.org/10.30546/224578.010.2025.015

Abstract

Currently, in various jurisdictions and unions, legislation on cryptocurrencies remains insufficiently adapted to respond to the constantly evolving threats that undermine the foundations of the cryptosphere. The lack of standardisation of laws, both domestically and internationally, contributes to the weakness and fragmentation of existing regulatory frameworks. In response to these shortcomings, this paper aims to propose a guiding framework for a global legal structure. The main objective of the proposal is to minimise the complexities arising from the interaction of multiple legal systems in cross-border cryptocurrency-related insolvency cases and, consequently, to reduce the overall number of such insolvencies. The paper also highlights the existing differences between developed and developing countries in terms of legal implementation, emphasising the importance of designing simpler and more practical legislative approaches for developing countries, particularly given their resource constraints. Furthermore, the paper analyses the legal frameworks of six different jurisdictions – the United States, the United Kingdom, the European Union, France, Kenya, and Singapore, and evaluates their effectiveness in managing risks associated with cryptocurrencies. It also presents specific recommendations and guiding principles addressing four major risks: market manipulation, partially backed stablecoins, money laundering and terrorist financing, and theft. A comparative analysis of the legal frameworks of these jurisdictions is conducted for each of these risks, identifying where current regulations fall short in addressing these threats. Finally, the paper provides targeted proposals for each risk area, contributing to the broader goal of promoting greater global standardisation of cryptocurrency legislation.

Annotasiya

Hazırda müxtəlif yurisdiksiyalarda və ittifaqlarda kriptovalyutalarla bağlı qanunvericilik kriptosferanın əsasını sarsıdan, daim dəyişən təhdidlərə cavab vermək baxımından kifayət qədər uyğunlaşdırılmayıb. Qanunvericiliyin həm daxili, həm də beynəlxalq səviyyədə standartlaşdırılmamasının özü də tənzimləmələrin yetərincə möhkəm və hərtərəfli olmamasına gətirib çıxarır. Bu çatışmazlıqlara cavab olaraq, məqalə qlobal hüquqi çərçivə üçün istiqamətverici bir təklif irəli sürməyi qarşısına məqsəd qoyur. Təklifin əsas məqsədi kriptovalyuta bazalı transsərhəd iflas hallarında bir neçə hüquqi çərçivəyə istinad etməklə yaranan mürəkkəblikləri azaltmaq və nəticə etibarilə iflas hallarının sayını minimuma endirməkdir. Məqalədə inkişaf etmiş ölkələrlə inkişaf etməkdə olan ölkələr arasında qanunların tətbiqi baxımından mövcud fərqlər də vurğulanır və xüsusilə resurs çatışmazlığı səbəbilə inkişaf etməkdə olan ölkələr üçün daha sadə və praktik qanunvericilik yanaşmalarının hazırlanmasının vacibliyi önə çəkilir. Daha sonra altı fərqli yurisdiksiyanın: ABŞ, Böyük Britaniya, Avropa İttifaqı, Fransa, Keniya və Sinqapurun qanunvericilik çərçivələri təhlil olunur və onların kriptovalyutalarla bağlı risklərin idarə edilməsində effektivliyi qiymətləndirilir. Məqalədə həmçinin bazar manipulyasiyası, qismən

[*] 2nd year student at Hwa Chong Junior College.

təmin edilmiş stabilkoinlər, çirkli pulların yuyulması və terrorizmin maliyyələşdirilməsi, habelə oğurluq kimi 4 əsas risk üzrə xüsusi təkliflər və istiqamətverici qaydalar təqdim edilir, bu risklərlə bağlı müxtəlif yurisdiksiyaların hüquqi çərçivələrinin müqayisəli təhlili aparılır və mövcud qanunvericiliklərin qeyd olunan təhdidlərə qarşı yetərsiz qaldığı məqamlar vurğulanır. Əlavə olaraq, hər bir risk üzrə xüsusi təkliflər təqdim edilir ki, bu da qlobal qanunvericiliyin daha çox standartlaşdırılmasına xidmət edir.

CONTENTS

Introduction

The 2014 hack of the Mt. Gox Bitcoin base saw the loss of $450M USD in assets after the theft of approximately 850000 BTC.[1] Specifically, the breach was a result of security vulnerabilities within Mt. Gox's digital infrastructure, which hackers had exploited to gain access to the base's wallet system. Without sufficient funds to repay creditors for their losses, the company eventually filed for bankruptcy. The insolvency proceedings that followed were a *locus classicus* for understanding the risks associated with cryptocurrencies, and the repercussions of the inadequate regulatory structures that govern them.

Today, the collapse of Mt. Gox remains significant because it brought three main issues into sharp focus: first, the insufficiency of compensation for creditors; second, jurisdictional issues regarding the process of obtaining remuneration; and third, differences in the classification of cryptocurrencies across different jurisdictions. The first highlights the extent of losses following the insolvency of a cryptocurrency base: since most cryptocurrency bases handle a relatively large sum of cryptocurrencies,[2] their insolvency would result in creditors suffering huge financial losses. In the case of Mt. Gox, the Bitcoin base had insufficient reserves to compensate platform users for their losses, and could no longer remain solvent. During the course of the proceedings, overseas creditors had to seek remuneration via the Japanese legal system – one that, at the time, lacked a robust regulatory framework for cryptocurrencies.[3] The substantial sum of assets lost by creditors, in addition to the cumbersome process of obtaining restitution, underscored the lack of comprehensiveness of current legislation. By contrast, the latter two issues pertained not to the insufficiencies of individual frameworks, but to the lack of a standardised global framework facilitating cross-border cooperation. Beyond the difficulty of obtaining remuneration, since creditors had to seek restitution under the Japanese legal system, the lack of cross-border coordination to address risks related to cryptocurrencies was pinpointed as a major flaw in legislative efforts.[4] Mt. Gox, it may be argued, was the catalyst for new legislative efforts surrounding cryptocurrencies due to its illustration of the heightened risks that cryptocurrencies carry, as well as the implications of these risks for possible cases of insolvency.

---

[1] Insolvency (2020), https://www.law.cornell.edu/wex/insolvency (last visited Aug. 28, 2025).

[2] Lennart Ante & Ingo Fiedler, *Market Reaction to Large Transfers on the Bitcoin Blockchain - Do Size and Motive Matter?*, 39 Finance Research Letters, Article 101619 (2021).

[3] Thomas Burgess, *A Multi-Jurisdictional Perspective: To What Extent Can Cryptocurrency be Regulated? And if so, Who Should Regulate Cryptocurrency?*, 5 Journal of Economic Criminology, Article 100086 (2024).

[4] Mai Ishikawa, *Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case*, 3 Journal of Financial Regulation 125, 126 (2017).

Consequently, attempts at enacting more robust legislation were observed across different jurisdictions in the wake of Mt. Gox. Different countries now recognised the importance of addressing the risks of cryptocurrencies in order to reduce the chances of insolvency – the term loosely defined as a debtor's inability to repay the debts they owe.[5] Considering the fact that Mt. Gox led to an overall depression in the prices of other cryptocurrencies,[6] in turn affecting the overall cryptocurrency ecosystem, it is evidently in a state's interest to prevent the insolvency of its cryptocurrency bases. A study by Khan et al. using the Bayesian structural model further illustrated the causal effect of the futures exchange insolvency on other major cryptocurrencies like Solana,[7] emphasising how insolvency events can have systemic impacts, including the depression of market values. It is therefore of great primacy for a state to enact legislation governing the risks of cryptocurrencies, given that their volatile nature can easily trigger such insolvency events.

Yet today, the efficacy of these frameworks is complicated due to the fragmented classification of cryptocurrencies in different jurisdictions. The decentralised nature of cryptocurrencies means that they are cross-border assets – they do not belong to any particular jurisdiction. If two jurisdictions were to regulate cryptocurrencies differently, then the insufficiencies of both legislations could be capitalised on by international criminal groups. After all, cryptocurrencies present heightened risks in financial markets, and should be regulated in a robust and standardised manner.

In this paper, I will discuss four of these risks – namely, market manipulation, partially backed reserves, money laundering/terrorism financing and theft, as well as suggest potential legislative measures that may be implemented by jurisdictions to mitigate them. I propose that these measures be enacted under a global legal framework so as to provide some standardisation to the currently fragmented legislation.

I. Cryptocurrencies: Risks and Rewards

To understand the risks of cryptocurrencies, it is important to first understand what traits of cryptocurrencies make them so volatile. In this regard, it is apposite to address the historical genesis of cryptocurrencies and explain why they have received such widespread uptake.

The conception of Bitcoin arguably the face of cryptocurrency itself came as a response to the 2008-2009 Global Financial Crisis. The Crisis, which saw

[5] Rick Maeda, State of the Japanese Crypto Market (2024), https://www.prestolabs.io/research/state-of-the-japanese-crypto-market (last visited Oct. 15, 2025).

[6] Sandeep Rao, Mt. Gox – The Fall of a Giant, in *Understanding Crypto Fraud, in Understanding Cryptocurrency Fraud: The Challenges and Headwinds to Regulate Digital Currencies* 71, 78 (2022).

[7] Khalid Khan, Adnan Khurshid & Javier Cifuentes-Faura, *Causal Estimation of FTX Collapse on Cryptocurrency: A Counterfactual Prediction Analysis,* 11 Financial Innovation, Article 16 (2025).

the collapse of the Lehman Brothers and other major financial institutions, was, to the masses, a consequence of the Federal Reserve's failure to secure adequate funding to ensure their solvency.[8] In an era plagued by sentiments of distrust in the banking system and government intervention, cryptocurrencies provided a beguiling solution: a decentralised system where transactions flow directly from one user to another, without the need for a central intermediary.

As defined in a PwC report, a cryptocurrency is a "digital medium of exchange that uses cryptographic techniques to verify the transfer of funds and control the creation of monetary units".[9] Its inimitability lies in its use of blockchain technology, which involves recording transactions as a series of "blocks", each of which contains a list of verified transactions. Because blockchains are encrypted, many users also exalt the technology as a way to engage in secure transactions that cannot be tampered with: for instance, blockchain technology eliminates the risk of "bitcoin misuse such as double spending" by providing a "verifiable record of transactions".[10]

The system further provides a sanctuary of privacy: in an age of increased government surveillance, it provides a platform for users to engage in pseudonymous transactions. Blockchains like Monero and Zcash have implemented built-in privacy features which enhance the confidentiality of transactions,[11] in line with the original intention of cryptocurrencies to serve as a platform for unsurveilled transactions.

Nonetheless, cryptocurrency does not lack in its detractors: many approach the sector with caution due to the various risks associated with it money laundering, market manipulation, and financial instability, to name a few. Within the span of the last decade, the world has seen massive blows to the industry, such as, *inter alia*, Tornado Cash being implicated in the laundering of $7B USD worth of cryptocurrency,[12] and Luna losing $60B USD from the

[8] Government Failure Caused the Financial Crisis (2009), https://iea.org.uk/blog/government-failure-caused-the-financial-crisis (last visited Oct. 15, 2025).

[9] Making Sense of Bitcoin, Cryptocurrency and Blockchain (2016), https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html (last visited Oct. 19, 2025).

[10] Adiseshu Hari & T. V. Lakshman, The Internet Blockchain: A Distributed, Tamper-Resistant Transaction Framework for the Internet, (HotNets'16: Proceedings of the 15th ACM Workshop on Hot Topics in Networks, 2016), https://dl.acm.org/doi/10.1145/3005745.3005771.

[11] Sophie Christensen, A Comparative Study of Privacy-Preserving Cryptocurrencies: Monero and ZCash (5) (Master thesis, University of Birmingham) (2018).

[12] Xiong Xihan & Luo Junliang, Global Trends in Cryptocurrency Regulation: An Overview, in *Mathematical Research for Blokchain Economy* 71, 75 (2024).

2022 Terra-Luna crash.[13]

As much of recent literature has shown, the liquidation of these companies was largely attributable to the risks of cryptocurrencies. In the Terra-Luna collapse, for instance, the Terra stablecoin – a cryptocurrency intended to be pegged 1:1 to the USD – was only partially backed by USD reserves, relying instead on an algorithm related to the LUNA token for backing. Thus, when investors sold off their coins *en masse*, a liquidity crisis ensued as the algorithm failed to maintain the peg. From this, it is evident that the risks of cryptocurrencies are causally linked to the insolvency of cryptocurrency companies.

Consequently, many jurisdictions have set out to implement policies aimed at mitigating the aforementioned risks. Whilst a considerable number of jurisdictions have taken the draconian measure of completely banning cryptocurrencies, there are just as many jurisdictions that have taken a more optimistic approach. Notable examples include the United States, where legislators are looking to incorporate cryptocurrencies into existing legal frameworks, and the European Union, where legislators have created an entirely new legal framework to address cryptocurrencies.[14]

As mentioned earlier, this paper aims to investigate the risks of cryptocurrencies and how different jurisdictions have set out to address said risks. In doing so, the levels of sufficiency of current legal frameworks will be noted, and a corresponding guideline for a global legal framework will be proposed. The guideline aligns with the original purpose of cryptocurrencies by aiming to regulate them enough to reduce criminal activity without wholly diminishing the advantages of cryptocurrencies**.**

This paper focuses on six different jurisdictions: the United States, the United Kingdom, Kenya, the European Union, France and Singapore. Since these jurisdictions were chosen with a view to providing a guideline for a global legal framework, countries that have banned, or greatly restricted the use of, cryptocurrencies have been excluded from this paper. After all, they would be unlikely to partake in a global framework or to have any significant legislation worth discussing. Out of the six focus jurisdictions, five were chosen for their robust regulatory frameworks, as these frameworks would provide a good foundation for a global framework and require few tweaks. Firstly, the choices of the US and UK are attributable to their comprehensive legislation concomitant with their large number of crypto investors, exchanges, and related platforms. The EU and France have also implemented

[13] What Really Happened to LUNA Crypto? (2022), https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/ (last visited Oct. 15, 2025).

[14] *See* The Law Library of Congress, Regulation of Cryptocurrency around the World (2018). Available at: https://tile.loc.gov/storage-services/service/ll/llglrd/2018298387/2018298387.pdf (last visited Oct. 8, 2025).

bespoke frameworks, with the EU's MiCA Regulation being the world's first legal framework specific to cryptocurrencies.[15] Singapore's regulations are not lacking in merits either the country is becoming a crypto hub, with 13 crypto licenses issued in 2024.[16] By contrast, the final jurisdiction selected for this paper has notably issued warnings about the risks of cryptocurrencies to its citizens: in this respect, Kenya may seem opposed to the adoption of cryptocurrencies. However, a rising trend of cryptocurrency adoption among Kenyan youth has emerged,[17] while the aforementioned warnings are largely due to Kenya's sparse regulatory frameworks for cryptocurrencies. I posit that Kenya's seeming aversion to cryptocurrencies is only due to its prioritisation of bread and butter issues, a situation that arises from its status as a developing country. Hence, Kenya was chosen as the final jurisdiction, as it can allow for a comparison between higher and lower income countries, which would be an important point of consideration for a global framework.

II. The Necessity of a Global Legal Framework

Finally, the hefty project of proposing a global legal framework has been undertaken in this paper. A global legal framework is necessary primarily because the marked discrepancies between different jurisdictions' legal frameworks engender an inefficient legal process, exacerbating the risks associated with cryptocurrencies.

A global legal framework is primarily needed to expedite the legal and regulatory processes concerning cryptocurrency firms. As discussed previously, different jurisdictions can classify cryptocurrencies very differently, with some treating them as property for tax purposes, and others having yet to establish a clear classification. This incongruence introduces significant compliance challenges to cryptocurrency exchanges with establishments in different jurisdictions, as they would be required to enact different internal frameworks depending on each jurisdiction's classification of cryptocurrencies.

This is evidenced in the 2020 case *SEC v. Ripple Labs Inc.*, where the U.S. Securities and Exchange Commission (hereinafter SEC) filed a lawsuit against cryptocurrency company Ripple Labs for conducting an unregistered

[15] Anne-Gaëlle Delabye, EU Parliament Adopts MiCA - the Key Points (2023), https://www.ogier.com/news-and-insights/insights/eu-parliament-adopts-mica-the-key-points/ (last visited Oct. 8, 2025).

[16] Singapore Pulls Ahead of Hong Kong in Race to be Crypto Hub (2024), https://www.businesstimes.com.sg/companies-markets/banking-finance/singapore-pulls-ahead-hong-kong-race-be-crypto-hub (last visited Apr. 24, 2025).

[17] Abubakar Nur Khalil, Kenyan Youth Embrace Bitcoin Amid Deadly Protests Over Finance Bill (2024), https://www.forbes.com/sites/digital-assets/2024/06/26/kenyan-youth-embrace-bitcoin-amid-deadly-protests-over-finance-bill/ (last visited Oct. 8, 2025).

securities offering.[18] The SEC claimed that Ripple had sold its tokens (XRP tokens) to investors, transgressing the provisions of the SEC's security laws. However, Ripple argued that XRP should instead be classified as a currency due to its primary use as a medium of exchange. Though the case is still ongoing, it is of note that the other jurisdictions Ripple has establishments in generally do not classify cryptocurrencies as securities, or only classify a small subset of cryptocurrencies as securities. For instance, Japan, which is set to adopt XRP in all of its banks in 2025, mostly classifies cryptocurrencies as a form of property under the Payment Services Act.[19] Thus, if the court rules in the SEC's favour, Ripple would be forced to adopt differing internal regulatory requirements across different jurisdictions, which would encumber the compliance process.

Even within jurisdictions, there may be no standardised classification of cryptocurrencies: the United States, for instance, classifies cryptocurrencies differently according to which regulatory body they fall under. Specifically, cryptocurrencies would be considered securities under the SEC, property under the Internal Revenue Service, and commodities under the Commodity Futures Trading Commission (hereinafter CTFC). Though this range of classifications provides more frameworks to regulate cryptocurrencies, it makes the classification very case-specific, which may lead to confusion for businesses. Coinbase, a US-based cryptocurrency exchange, encountered this problem when it released its Lend program in 2021: the SEC sent a Wells notice to Coinbase after its announcement, stating that the product could constitute an illegal securities offering.[20] Subsequently, Coinbase was forced to pause this rollout and engage in costly legal discussions over the classification of its product. As illustrated, the lack of clarity in whether a cryptocurrency is classified as a security, commodity or property creates a significant administrative burden on companies. This further introduces compliance challenges, underscoring the need for a synthesised legal framework.

Ultimately, such compliance challenges could lead to a misstep on a company's part due to the complicated nature of the fragmented legislation governing its international operations. If a company were to fail to implement a new set of legislation enacted in only one jurisdiction, it might become a target for criminals in the cryptosphere. As a result, a company might be more

[18] Securities and Exchange Commission v. Ripple Labs Inc., 2d Cir. No. 24-2648 (2024). Available at: https://www.courtlistener.com/docket/69230851/securities-and-exchange-commission-v-ripple-labs-inc/ (last visited Oct. 6, 2025).

[19] Japan and Cryptocurrency (2021), https://freemanlaw.com/cryptocurrency/japan/ (last visited Oct. 15, 2025).

[20] Todd Ehret, SEC Spat with Coinbase Previews Complex Legal Battle over Crypto (2021), https://www.reuters.com/legal/transactional/sec-spat-with-coinbase-previews-complex-legal-battle-over-crypto-2021-09-28/ (last visited Oct. 5, 2025).

susceptible to the risks of cryptocurrencies and therefore be more susceptible to insolvency. In the case of Ripple Labs, the high-profile nature of the case would create high visibility for companies and independent entities, allowing them to capitalise on Ripple Lab's sale of its tokens. While other companies would have enacted legislation against this, Ripple Lab's lack of a similar internal regulation on the sale of its tokens might allow for companies or independent entities to purchase a large sum of tokens, resulting in potential abuses in the form of market manipulation. As will be explicated later, this can in turn lead to a company's insolvency via pump and dump schemes. Accordingly, it is important to enact uniform legislation across jurisdictions such that companies with international operations face less compliance challenges and can better safeguard against the risks of cryptocurrencies.

Nonetheless, while the primary goal of a global legal framework is the increased efficiency of legal processes, it can also allow different jurisdictions to be more on par with each other, regardless of their socioeconomic statuses. This would, in turn, prevent developing countries from being exploited by criminals due to their less robust legislative frameworks. It would be useful to refer back to an issue that was raised earlier: compared to the other five jurisdictions discussed in this paper, Kenya has a far less bespoke legal framework to govern cryptocurrencies. This is in part due to its status as a developing country, which reflects the more pressing issues its government needs to address through legislation. However, as the National Security Council asserts, transnational organised crime often penetrates developing countries with weak legislative frameworks,[21] making Kenya all the more susceptible to threats in the cryptosphere.

A global legal framework has the potential to counter this by including provisions on information sharing or cybersecurity support for developing countries, it can allow these countries to adopt stronger legislation without the associated costs. In addition to strengthening the global response to the threats of cryptocurrencies, a global framework will also allow developing countries to progress alongside developed countries, or at least, narrow the gap between the two. This can foster more equitable progress by lessening the socioeconomic divide between countries, and paving the way for new opportunities within developing nations. For instance, given the increased interest in Bitcoin among Kenyan youth,[22] a global legal framework could accelerate the development of Kenya's cryptocurrency sector and encourage more youths to enter into it.

Finally, it is worth noting that regional regulatory frameworks are already in place to address the threats of cryptocurrencies, offering comprehensive

[21] Transnational Organized Crime: A Growing Threat to National and International Security (2021), https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat (last visited Feb. 25, 2025).

[22] Khalil, *supra* note 17.

measures that enhance the regulatory frameworks of participating jurisdictions. The MiCAR, for instance, is touted as a leading framework for cryptocurrencies, owing to its ability to "*remove regulatory barriers for dealing with crypto assets*".[23] This, in turn, can provide EU member states with a largely standardised framework to address cryptocurrencies. As Gijs op de Weegh, CEO of stablecoin platform StabIR, asserts, MiCAR's success could set a global regulatory precedent,[24] allowing the benefits of a regional framework to be extended to the rest of the world.

Ergo, with the current misalignments in the legal frameworks of different jurisdictions, a global legal framework is unequivocally necessary. Beyond strengthening the global response to the threats of cryptocurrencies, it can provide more equitable progress in developing countries and streamline insolvency proceedings. Ultimately, such a framework aims to promote more widespread adoption of cryptocurrencies due to their myriad of benefits, while nonetheless mitigating the threats associated with them.

III. From Soft Law to Hard Law: Guidelines for a Global Legal Framework

Before delving into the specific risks of cryptocurrencies, I begin by emphasising that the final goal of the guidelines set out below is the creation of a legally binding global framework. In this respect, the framework mirrors the various frameworks that govern international trade under the World Trade Organisation (hereinafter WTO) in the sense that it will have an intergovernmental treaty of rights and obligations among its signatories.[25] In particular, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, an agreement under the broader Marrakesh Agreement establishing the WTO is cited.[26] By focusing solely on the effects of such an agreement, we can better appreciate its effectiveness as compared to if it were a non-legally binding framework: after the TRIPS Agreement was signed in 1994, it came into force for developed countries in 1995.[27] Signatories

[23] Renato Fazzone & Susana Esteban, MiCAR: An Overview of Everything Important about the Crypto Regulatory Framework (2023), https://www.ftitechnology.com/resources/blog/micar-an-overview-of-everything-important-about-the-crypto-regulatory-framework (last visited Oct. 6, 2025).

[24] Exploring the Impact of MiCAR on European Stablecoins: Gijs op de Weegh's Insightful Opinion on Blockworks (2024), https://www.stablr.com/insights/exploring-the-impact-of-micar-on-european-stablecoins-gijs-op-de-weeghs-insightful-opinion-on-blockworks (last visited Oct. 15, 2025).

[25] Rorden Wilkinson, *The World Trade Organization,* 7 New Political Economy 129, 133 (2002).

[26] *See* Peter Van den Bossche, Economic Globalisation and the Law of the WTO, in *The Law and Policy of the World Trade Organization* 1 (2012).

[27] Arno Hold & Bryan Mercurio, *Transitioning to Intellectual Property: How Can the WTO Integrate Least-Developed Countries into TRIPS?* 7 (NCCR, Working Paper No. 2012/37, 2012).

were required to implement its laws into their domestic legal frameworks, which allowed for full compliance with rigorous international regulations. By contrast, if the agreement operated under a non-legally binding framework, countries would lack the same incentive to adopt its provisions unless absolutely necessary. This would result in significant disparities between the legal systems of different countries, further complicating cross-border legal issues. As evidenced, a legally binding global framework is crucial to ensuring compliance with global best practices, as it places pressure on countries to conform, rather than allowing them the flexibility to implement such laws at their own pace.

However, legally binding global frameworks are admittedly cumbersome to implement, and may take a long time to come into force. Referencing the TRIPS Agreement, discussions surrounding its development began in 1986 during the Uruguay Round, and it was only implemented in developing countries by 2000.[28] In the context of cryptocurrencies, countries simply do not have the luxury of time to wait for the implementation of a legally binding global framework. Rather, global best practices must first be integrated into domestic laws to counter imminent threats to the cryptosphere.

This may be achieved through the provision of a single global standard for cryptocurrencies, rather than the fragmented frameworks presently adopted to address different areas of threats. While it is best to implement a legally binding framework, this would take significantly longer as compared to implementing a non-binding framework. Therefore, rather than waiting for a legally binding framework to be implemented, it is important that a non-binding framework be implemented in the interim.

While it remains a limitation that countries may be less likely to adopt global best practices under a non-binding framework, this does not imply that a global standard is completely ineffective: the implementation of the FATF Recommendations, the UNCITRAL Model Law on Cross-Border Insolvency, and MiCAR in various countries has spurred significant progress in addressing the risks posed by cryptocurrencies.[29] By aligning their domestic legislation with best practices and addressing the gaps set out in this paper, countries will be able to bolster their defences against threats to the cryptosphere.

That said, the largest drawback of a global standard is its potential lack of adoption in developing countries. Due to their focus on more pressing issues like housing or food shortages, these countries may lack the resources to implement costly and specialised compliance measures, engendering a significant gap between the legislation of developed and developing nations.

[28] Wilkinson, *supra* note 25, 129.

[29] *See* Financial Stability Board, G20 Crypto-Asset Policy Implementation Roadmap: Status Report (2024). Available at: https://www.fsb.org/uploads/P221024-3.pdf (last visited Oct. 8, 2025).

Nonetheless, this limitation may be addressed via intervention from large international organisations like the UN, which could provide funding or global aid to support developing countries in implementing such frameworks.

In summary, the guidelines delineated below are, first and foremost, intended as a short-term guide for countries to implement best practices under a non-binding standardised framework. Developing countries may be limited in their capabilities to adopt such frameworks, which calls for the need for global intervention. However, in the long term, it is imperative for a legally binding global framework to be implemented in order to ensure that signatories are compliant with a unified and robust framework.

The following sections explicate the four primary risks of cryptocurrencies, as well as outline the insufficiencies in the approaches various jurisdictions have adopted to address these risks. Potential solutions to these insufficiencies are then proposed alongside an explanation of how the legislation discussed may be integrated into a global legal framework.

IV. Market Manipulation

A. Overview of Risk

The threat market manipulation poses to cryptocurrency platforms has been a sustained topic of inquiry in cryptocurrency discussions, underscoring the importance of suitable regulation. But with the current lack of regulation on cryptocurrency exchanges and traders, this threat can manifest itself in two forms: first, as a result of the fraudulent activity of cryptocurrency exchanges, and second, as a result of gaming by organised trading groups. This section instantiates the first form of market manipulation with a case study centered on Tether and Bitfinex, and discusses the lack of regulation on this front. The second form of market manipulation will only be summarised briefly as it is highly technical and can be addressed by other blanket regulations.

Controversy and claims of market manipulation have long surrounded the relationship between Bitfinex, a cryptocurrency base, and Tether, a stablecoin (USDT). As John Griffin and Amin Shams assert in their paper, the stablecoin Tether is supply-driven, or "pushed", meaning that it is printed regardless of demand.[30] This "push" mechanism can result in an additional supply of Tether circulating in the crypto space, creating an artificial demand for cryptocurrencies like Bitcoin due to greater perceived liquidity or market activity. This incentivises investors to purchase a larger sum of the cryptocurrencies, which in turn inflates their prices. These findings, and their implications of market manipulation, are reified in the fact that both of the

[30] John M. Griffin & Amin Shams, *Is Bitcoin Really Un-Tethered?*, 75 The Journal of Finance 1913, 1915 (2020).

aforementioned companies (Bitfinex and Tether) are operated by iFinex Inc.[31]. This raises the question of whether the two have ever colluded to manipulate the cryptocurrency market: for instance, many critics have questioned whether Tether is fully-backed by fiat currencies. If Tether is supply-driven, and is printed regardless of demand, then the company must possess a large sum of fiat currency reserves in the event of mass redemptions. This is evidently highly unlikely, but even if Tether is fully-backed, a further question arises as to how it has obtained such a large collateral.

Setting aside the first question for now, this section considers a theory posited by the blogger Bitfinex'ed:[32] in February of 2018, he detailed a scenario where Tether, first issues large sums of USDT to buy other cryptocurrencies on Tether-supported cryptocurrency exchanges like Bitfinex, then transfers said cryptocurrencies to other cryptocurrency exchanges like GDAX to be converted into fiat currencies, which will subsequently be transferred back into the bank account of Tether. This counter-balances downturns in cryptocurrency prices, but may backfire if a price correction occurs.

Ultimately, if artificially inflated cryptocurrency prices return to their normal values, this could lead to substantial losses, or even the insolvency, of companies engaging in market manipulation. For instance, companies like Tether, with large reserves of cryptocurrencies, might see a plunge in the value of their reserves. A large enough drop in value would make it difficult for Tether to remain solvent, and creditors would also lose much of their investments.

Other forms of market manipulation more closely associated with independent trading groups can have similar effects: pump and dumps, the acquisition of large amounts of a cryptocurrency asset followed by its promotion ("pumps") and sale ("dump"), can cause large drops in cryptocurrency prices.[33] In turn, this could possibly culminate in the liquidation of a cryptocurrency base. Nonetheless, "bottom-up" schemes like these are far less likely to result in insolvency, and tend to result in the losses of smaller capital.

B. Cross-Jurisdictional Analysis

This section reflects a comparative analysis of the six jurisdictions' legislative frameworks. The analysis will first tackle the United States, the United Kingdom and Singapore, since their legislation is relatively similar

[31] Tether: Overview, History, Stablecoins, Supply, https://corporatefinanceinstitute.com/resources/cryptocurrency/tether/ (last visited Aug. 15, 2025).

[32] Bitfinex'ed, Bitfinex and Tether is Unauditable: Why They will Never Do a Real Audit (2018), https://bitfinexed.medium.com/bitfinex-and-tether-is-unauditable-why-they-will-never-do-a-real-audit-3324e002b185 (last visited Oct. 8, 2025).

[33] "Pump and Dump" Schemes (2006), https://share.google/Sv5ik6zSrLC8jlEtg (last visited Oct. 7, 2025).

with regard to market manipulation. Thereafter, the regulatory frameworks enacted in the EU and France will be explained, followed by those in Kenya.

In the United States, the threat of market manipulation is governed by 3 regulatory bodies: SEC, CFTC, and the Federal Trade Commission (hereinafter FTC).

Firstly, the SEC governs any cryptocurrencies which fall under the category of securities. The 1946 Supreme Court case *SEC v. Howey Co.*[34] provides a lucid 4-point framework to ascertain whether an asset is considered a security: (1) There must be an investment of money by a party. (2) The party must be in a common enterprise. (3) The party must have the expectation of profiting. (4) The aforementioned expectation has to be based on the efforts of a third party. If a cryptocurrency fulfils this criteria, it will fall under the SEC's jurisdiction, and its cryptocurrency exchange will be mandated to comply with the Securities Exchange Act of 1934. The Act in question prohibits illicit practices like insider trading and market manipulation, which would, *a fortiori*, prevent individuals from engaging in manipulative market strategies. Should such a circumstance arise, however, the SEC would likely be able to detect unusual price spikes, given its established mechanisms to monitor market activity.

To exemplify, a cryptocurrency exchange engaging in manipulative practices can be charged for violation of section 10(b)-5 of the Act, which states that:

"*It shall be unlawful for any person to use or employ, in connection with the purchase or sale of any security registered on a national securities exchange [...], any manipulative or deceptive device [that runs contrary to public interest]*".[35]

Evidently, any individual engaging in manipulative strategies like pumps and dumps would be flagged out by the SEC as engaging in an unlawful practice.

Next, the CFTC enacted the Commodities Exchange Act (hereinafter CEA) in 1936 to enforce rules against market manipulation. Final Rule 180.2 of the CEA was modelled after the SEC's Rule 10(b)-5, and similarly prevents individuals from manipulating the market.[36] Nonetheless, its scope is broader than the SEC's Securities Exchange Act: it applies to any person involved in commodity transactions, whether or not they are registered under a particular exchange. Hence, a cryptocurrency exchange itself, or other unregistered participants, can also be implicated under the CEA. For instance, a cryptocurrency exchange that engages in the practice of minting new tokens to inflate market prices would likely be in violation of the Act such a practice would cause creditors to lose a large sum of investments after inflated prices return to normal, which would again be delineated by the CFTC as unlawful.

[34] SEC v. W.J. Howey Co., U.S. No. 843, (1946). Available at: https://supreme.justia.com/cases/federal/us/328/293/ (last visited Oct. 7, 2025).

[35] 15 U.S.C. § 78a.

[36] 7 U.S.C. § 1.

Finally, the FTC does not specifically regulate market manipulation, but has blanket rules under the 1914 FTC Act to prevent unfair or deceptive practices. Section 5 of the Act states that "*all persons engaged in commerce" are "prohibited from engaging in unfair or deceptive practices*".[37] Broadly speaking, this governs the executive board of cryptocurrency exchanges and condemns all manipulative practices, including methods to inflate market prices.

In the UK, the threat of market manipulation is primarily governed by the Financial Conduct Authority (hereinafter FCA). As detailed by Section 1.3.2 of the FCA Handbook, any person engaging in "*a transaction for a person's own benefit, on the basis of and ahead of an order [...] which he is to carry out with or for another [...], which takes advantage of the anticipated impact of the order on the market*" is considered to be taking part in insider trading, a form of market manipulation.[38]

Such a circumstance could arise if a cryptocurrency platform were to unlawfully mint new tokens with the intention to inflate market prices individuals with knowledge of this would be able to place trades based on anticipated price movements. Any such illicit activities, if detected, would then be governed by the Financial Services and Markets Act (FSMA), which the FCA handbook operates in conjunction with.

The provisions of the FSMA, whilst not specifically directed at cryptocurrencies, can extend to cryptoassets if they are deemed to be financial instruments. As defined by Section 102A of the FSMA, a financial instrument can be, *inter alia*, any form of "transferable security".[39] Therefore, any cryptocurrency classified as a security would fall under the jurisdiction of the FSMA. Further delving into the FSMA's legislation on market manipulation, Section 118(1) of the Act describes different forms of market manipulation – notably, *"behaviour [that] consists of effecting transactions or orders to trade which give, or are likely to give, a false impression as to [...] the price of one or more qualifying investments"*[40] is labelled a form of market manipulation. The quote above encapsulates how a cryptocurrency base may mint new tokens in order to inflate prices across the market. These artificially raised prices are, in turn, accounted for and governed by the FSMA's regulations.

In Singapore, the Monetary Authority of Singapore (hereinafter MAS) has introduced various pieces of legislation to counter the threat of market manipulation, including the Securities and Futures Act (hereinafter SFA) and the Consumer Protection (Fair Trading) Act. Additionally, the MAS has

[37] *Supra* note 35, § 41.

[38] Financial Conduct Authority, Handbook Notice 3, (2013). Available at: https://www.fca.org.uk/publication/handbook/fca-handbook-notice-03.pdf (last visited May 16, 2025).

[39] Financial Services and Markets Act, Section 102A (2000). Available at: https://www.legislation.gov.uk/ukpga/2000/8/section/102A (last visited Oct. 3 2025)

[40] *Id.*, Section 118 (1).

issued guidelines for cryptocurrency exchanges which, while not legally binding, provide a good framework for cryptocurrency firms to adhere to.

Under Section 17 of the SFA, a securities exchange must ensure that all systems in place for the purposes of risk management are "*adequate and appropriate for the scale and nature of its operations*".[41] This mandate, if contravened, is punishable by law, providing punitive motivation for companies to establish robust frameworks to safeguard against market manipulation on an individual level. However, this Act is limited in 3 aspects: first, it only pertains to cryptocurrencies classified as securities rather than cryptocurrencies in general; second, it only addresses market manipulation on an individual level, rather than addressing the threat of a company engaging in this practice; and third, its phrasing is far too broad to encompass the specific cybersecurity measures required to combat the threat of market manipulation. Section 3.4.2 of the MAS's guidelines for Digital Payment Token Providers (DPT Providers) is similarly constrained by the requirement for Providers to implement risk management systems to safeguard its customers' assets.[42] In response to these insufficiencies, the approaches delineated in the discussions section of this paper should be adopted accordingly. Besides the SFA, Singapore's Consumer Protection (Fair Trading) Act also addresses the threat of market manipulation in the cryptosphere. Similar to Kenya's Consumer Protection Act outlawing any false and misleading representations, Section 4 of this Act prohibits suppliers from engaging in any practices which would result in their customers being misled.[43] In the case of market manipulation, a company's artificial inflation of market prices could be penalised under this section of the Act, since it would mislead customers into believing that there is high demand for a certain token. However, there are no mandatory disclosure requirements for cryptocurrency companies, and documents are only required to be produced in the event of an investigation. As such, cryptocurrency companies that can conceal their illicit practices will be able to evade certain checks.

The insufficiency that the acts of all three jurisdictions share is that they are not specifically designed to address cryptocurrencies, but rather have been extended to cover cryptocurrencies within their scope. As such, they are lacking in some respects as they fail to take into account certain properties of

[41] Monetary Authority of Singapore, The Securities and Futures Act, § 17 (2001). Available at: https://www.mas.gov.sg/regulation/acts/securities-and-futures-act (last visited Sep. 21, 2025).

[42] Monetary Authority of Singapore, Guidelines on Consumer Protection Measures by Digital Payment Token Service Providers, Section 3.4.2 (2024). Available at: https://www.mas.gov.sg/regulation/guidelines/ps-g03-guidelines-on-consumer-protection-measures-by-dpt-service-providers (last visited Sep. 15, 2025).

[43] *See* Consumer Protection (Fair Trading) Act (2003). Available at: https://sso.agc.gov.sg/act/cpfta2003 (last visited Sep. 23, 2025).

cryptocurrencies, which are markedly different from traditional commodities. The property that features most prominently in this case is the difficulty of surveillance[44] a cryptocurrency base might fall under suspicion for market manipulation, but without concrete evidence, regulatory bodies are not permitted to launch an investigation. For instance, no formal investigation was launched on Tether in the United States, despite suspicious market patterns, citing the need for more internal reporting. If transparency cannot be maintained via an external institution, then mandates should be put in place for the publication of internal reports by cryptocurrency bases. This will better allow for the elucidation of an exchange's practices.

Moving on to the EU and France, the threat of market manipulation is governed by two legal frameworks in the EU: the Markets in Financial Instruments Directive II (MiFID II) and the Market Abuse Regulation (hereinafter MAR), both of which fall under the regulatory oversight of the European Securities and Markets Authority (hereinafter ESMA).

Under subsection 3 of Article 16 of MiFID II, a firm shall fulfil organisational requirements so as to, *inter alia*, *"take into account any event that could materially affect the potential risk to the identified target market"*.[45] This can broadly be applied to cases of market manipulation, where the issuance of new cryptocurrencies could lead to an inflation of market prices. The MAR further defines market manipulation as the "*act of misleading the market through activities that manipulate market prices*",[46] which includes collusion to influence the supply or demand of financial instruments. This would apply to situations like the one involving Tether and Bitfinex, whereby two closely associated cryptocurrency companies are suspected of colluding to artificially inflate market prices.

However, though MiFID II is comprehensive in addressing *financial instruments*, it nonetheless presents gaps in its scope. Article 16, as well as the entirety of MiFID II, applies only to investment firms, meaning cryptocurrencies traded by exchanges would need to be classified as financial instruments. Consequently, any cryptocurrency exchanges falling outside of these constraints would not be regulated by MiFID II, allowing for easier participation in illicit activities.

The newly established Markets in Crypto-Assets Regulation (hereinafter MiCAR) provides a promising solution that specifically targets cryptoassets: chapter 2 of title V in MiCAR lists obligations to be followed by crypto-asset

[44] Chen Xuan et al., *Visual Analytics for Security Threats Detection in Ethereum Consensus Layer,* 27 Journal of Visualization 469, 471 (2024).

[45] Directive 2014/65/EU of the European Parliament and of the Council, art. 16.3 (2014). Available at: https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng (last visited May 22, 2025).

[46] Regulation (EU) No 596/2014 of the European Parliament and of the Council, art. 12 (2014). Available at: https://eur-lex.europa.eu/eli/reg/2014/596/oj/eng (last visited Jan. 5, 2025).

service providers (CASPs), including governance arrangements aimed at ensuring market integrity.[47] Clause 54 of the Regulation echoes this mandate, although specifics are not provided on how a CASP should structure its internal regulations. Beyond that, market manipulation on the level of individuals or groups is regulated through the collection of information of counterparties involved in cross-border trading activity. MiCAR's mandate facilitates the detection of market abuse practices such as wash trading,[48] thereby regulating market manipulation at the individual/group level.

However, despite MiCAR's relative comprehensiveness as a legal framework, a more detailed substantiation of the first 2 clauses in the previous paragraph would contribute to a more bespoke framework. In particular, one potential avenue for improvement could involve the mandatory reporting of cryptocurrency issuances to regulatory bodies, accompanied by an independent third party audit. This approach would provide more stringent requirements for CASPs, disallowing them from neglecting internal regulatory standards and engaging in illicit conduct.

In France, the Autorité des Marchés Financiers (hereinafter AMF) and the Autorité de Contrôle Prudentiel et de Résolution (hereinafter ACPR) are the two regulatory bodies with oversight over market manipulation practices. To counter this threat, the AMF has adapted rules from the EU's Market Abuse Regulation (MAR), as well as issued guidelines in line with those of the European Banking Authority (hereinafter EBA).

The 2019 AMF Policy on Digital Asset Service Providers (DASPs) requires that upon registration, all firms provide, *inter alia*, "*an audit report produced by one or more third parties with Qualified Information Systems Security Audit Service Providers (hereinafter PASSI) qualification*".[49] Specifically, the report will cover organisational audit and configuration audit, both of which are likely to encompass internal controls and systemic structures within the firm. This makes it more challenging for firms to engage in illicit activities, as any issuance of tokens without proper oversight (or other unlawful practices) would be identified in an audit report. Therefore, the policy promotes greater

[47] Markets in Crypto-Assets Regulation (MICA), https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica (last visited Jan. 25, 2025).

[48] *See* Mikolaj Barczentewicz & André de Gandara Gomes, *Crypto-Asset Market Abuse Under EU MiCA* (2024). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4375201; Lin William Cong et al., *Crypto Wash Trading* (2020). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3530220 (last visited Oct. 12, 2025).

[49] Autorité des Marchés Financiers (French Financial Markets Authority), Digital Assets Service Providers – Cybersecurity System of Requirements § 7(4) (2019). Available at: https://www.amf-france.org/sites/institutionnel/files/private/2023-08/Instruction%20DOC-2019-24%20Digital%20assets%20service%20providers%20%E2%80%93%20Cybersecurity%20system%20requirements.pdf (last visited May 7, 2025).

transparency in cryptocurrency firms' operations due to its indirect disclosure requirements.

Compared to the other five jurisdictions, Kenya has a far more underdeveloped framework to address the threat of market manipulation in the cryptosphere. While Kenya has no laws specific to cryptocurrencies, the Central Bank of Kenya (CBK) and the Capital Markets Authority (CMA) have applied existing laws originally used to regulate traditional markets to cryptocurrencies.

To begin, the Capital Markets Act indirectly addresses market manipulation by granting the CMA regulatory oversight over the securities market. Though the CBK or other financial authorities in Kenya have not explicitly classified cryptocurrencies as securities or, for that matter, classified cryptocurrencies, it would be prudent to consider extending the Capital Markets Act to cryptocurrencies. The only restriction Kenya has placed on the classification of cryptocurrencies thus far is that they are "not legal tender",[50] meaning that it is not beyond reach to govern cryptocurrencies *qua* securities under the Act. To delve into the particulars of this, section 22B of the Act accords the CMA with the authority to "*intervene in the operations of securities exchanges*" if market manipulation, or the threat of market manipulation, is detected.[51] Under this section, the CMA can suspend trading activities on a securities exchange, allowing for enough time to conduct investigations.

Though the law works well to regulate practices of market manipulation, it is based on the premise that authorities will first be able to detect these practices. In the case of cryptocurrencies, however, this premise does not hold: Kenya has not implemented any frameworks to detect market manipulation in the cryptosphere, and also has not introduced disclosure rules for cryptocurrency companies. As such, the detection of market manipulation on both the individual and company level is challenging, and more needs to be done to implement cyber surveillance measures.

The next Act that can potentially be extended to address the threat of market manipulation in the cryptosphere is Kenya's Consumer Protection Act (hereinafter CPA). As stipulated in the Consumer Protection Guidelines, which serve as a complement to the Act, any "*false and misleading representations*" made by a service provider to its customers will be subject to liability under this Act.[52] In the case of market manipulation by

[50] Central Bank of Kenya, Public Notice on Virtual Currencies Such as Bitcoin, 1 (2015). Available at: https://www.centralbank.go.ke/images/docs/media/Public_Notice_on_virtual_currencies_such_as_Bitcoin.pdf (last visited May 15, 2025).

[51] *See* Capital Markets Act (1989). Available at: https://www.kenyalaw.org/lex//actview.xql?actid=CAP.%20485A (last visited BLA 2025).

[52] *See* The Consumer Protection Act (2013). Available at: https://new.kenyalaw.org/akn/ke/act/2012/46/eng@2022-12-31 (last visited Aug. 5, 2025).

cryptocurrency bases (similar to the speculation around Tether), this clause might be extended to cryptocurrency companies when they fail to disclose that market prices are artificially inflated due to their illicit printing of new tokens.

Again, the CPA provides a robust framework that can be applied to cryptocurrencies, though it is unfortunate that most "*false and misleading representations*" in practices of market manipulation will not be detected anyway. As such, it is paramount that Kenya shores up its cybersecurity measures in response to illicit cryptocurrency practices.

Nonetheless, I wish to note here that Kenya does not adopt as welcoming an approach to cryptocurrencies as the other jurisdictions discussed. While no bans have been placed on cryptocurrencies, the Kenyan government has warned its citizens against the trading of virtual currencies due to the lack of regulation in Kenya.[53] I posit that the reasons for a lack of regulation is not that Kenya does not eventually wish to broaden its cryptocurrency market, but rather that there are more pressing issues which require resources to be addressed. This is evidenced in the fact that Kenya is classified as a developing country under the United Nations Development Program[54] its government needs to address the more fundamental needs of its citizens, such as by establishing a reliable power system,[55] before it can move to rapidly developing areas of technology. Thus, in the subsequent section of this paper (wherein I will propose a guideline for a global legal framework), due consideration will be given to financial subsidies for developing countries.

C. Recommendations for a Global Legal Framework

Of all the frameworks discussed, France's 2019 AMF Policy on Digital Asset Service Providers, as well as its other regulations borrowed from the EU, are perhaps the most robust in mitigating the risk of market manipulation in the cryptosphere. Specifically, France requires that upon registration, firms provide an audit report produced by a third party with PASSI qualifications. This mandate is notably absent from the other jurisdictions discussed in this paper, which decreases the transparency of a firm's internal operations. Given that market manipulation perpetuated by cryptocurrency firms themselves is particularly hard to detect, it is imperative to implement more stringent oversight measures to maintain internal controls and market integrity.

Accordingly, **(1)** *France's 2019 AMF Policy, as well as the EU's MAR and MiCA Regulation, should be referenced in creating a global legal framework*. This addresses

[53] *Supra* note 50.

[54] *See* United Nations Development Programme, Global Multidimensional Poverty Index 2024: Poverty Amid Conflict (2024). Available at: https://www.undp.org/sites/g/files/zskgke326/files/2024-10/2024_global_multidimensional_poverty_index.pdf (last visited May 21, 2025).

[55] *See* Mungai Kihara et al., *Mid- to Long-Term Capacity Planning for a Reliable Power System in Kenya,* 52 Energy Strategy Reviews 1 (2024).

the insufficiencies of other legal frameworks by allowing authorities to detect market manipulation more easily without having to expend resources to launch a formal investigation. To recapitulate, other jurisdictions like the US are not permitted to launch investigations without concrete evidence of market manipulation: under this framework, authorities will be able to obtain evidence in an expedient manner simply by analysing an audit report of a suspected firm. Therefore, French legislation is able to address the gaps in other jurisdictions' regulations and should be taken as a reference for the global framework.

Notwithstanding the boons of French legislation, there are still certain insufficiencies that no legal framework has addressed to date. France's AMF Policy requirements only apply to firms undergoing registration, and do not require annual third party audits for registered firms. This allows for potential market manipulation subsequent to a firm's registration, which may be addressed via **(2)** *the mandate that firms submit annual audit reports compiled by third parties to regulatory bodies*. Specifically, these audit reports should cover, *inter alia*, the minting of any new tokens, operational safeguards and internal controls.

In summary, the regulatory changes proposed are as follows: First, upon registration, firms must provide an audit report produced by a third party with PASSI qualifications (or the equivalent qualifications in other jurisdictions). This is to ensure maximum transparency in a firm's activities and prevent the illicit issuance of cryptocurrencies to inflate market prices. Additionally, firms must submit annual audit reports compiled by third parties to regulatory bodies. This allows for sustained oversight on any new issuances of a cryptocurrency firm.

V. Partially Backed Reserves

A. Overview of Risk

Following a similar tangent to market manipulation, another risk of cryptocurrencies specifically, stablecoins is the lack of full backing or adequate reserves to maintain their stability. Stablecoins can be "backed" by a variety of assets such as fiat currencies or cryptocurrencies, though some are only partially backed and instead use algorithms to maintain their stability.[56] Nevertheless, the most widely adopted backing system is that of fiat currencies, which is favoured for its ability to decrease the volatility of cryptoasset prices.

In recent years, much speculation has arisen about whether or not stablecoins are fully backed: critics argue that many stablecoin companies seem to lack adequate reserves, which could increase price volatility and

[56] *See* Christian Catalini, Alonso de Gortari, & Nihar Shah, *Some Simple Economics of Stablecoins*, 14 Annual Review of Financial Economics 117 (2022).

undermine the function of a stablecoin as a stable store of value.[57] Furthermore, if a stablecoin's lack of full backing is revealed to the public, this might result in a loss of trust in said stablecoin, causing investors to attempt to redeem their stablecoins for fiat currency *en masse*. A company lacking sufficient reserves of fiat currency would then need to sell its assets rapidly in order to handle large redemption requests, which could potentially lead to a liquidity crisis for companies without sufficient collateral.

The above is evidenced by the June 2021 collapse of the IRON stablecoin, a stablecoin designed to incorporate elements of both cryptocurrency-backed stablecoins and algorithmic ones.[58] Because of its reliance on an algorithm, IRON was only partially collateralised through a combination of the stablecoin USDC and its native token Titan.[59] However, after Titan experienced a large sell-off, its prices plummeted, causing IRON's algorithm to break down. Its peg to Titan could no longer be maintained, and investors hastened to redeem their IRON tokens for other assets, resulting in a large volume of sell-offs. Creditors who failed to act fast lost large sums of their investments, while IRON struggled to maintain enough liquid reserves to cover its liabilities. Eventually, the company was forced to enter a de facto insolvency.[60] This example accentuates two essential aspects of stablecoins that regulators should keep in mind: first, the high risk of insolvency that results from a lack of full backing, and second, the even more heightened risks of algorithmic stablecoins as compared to stablecoins using other forms of collateral. Therefore, it follows that further stablecoin collapses mirroring the liquidation of Iron Finance are bound to occur in jurisdictions lacking sufficient regulation, which underscores the need for comprehensive regulations.

B. Cross-Jurisdictional Analysis

In the United States, multiple regulatory bodies have proposed legislation to mitigate this risk. In particular, the Financial Stability Oversight Council (hereinafter FSOC)[61] monitors risks related to stablecoins, and the Stablecoin

[57] *See* G7 Working Group on Stablecoins, Investigating the Impact of Global Stablecoins (2019). Available at: https://www.bis.org/cpmi/publ/d187.pdf (last visited Jan. 22, 2025).

[58] Austin Adams & Markus Ibert, Runs on Algorithmic Stablecoins: Evidence from Iron, Titan, and Steel (2022), https://www.federalreserve.gov/econres/notes/feds-notes/runs-on-algorithmic-stablecoins-evidence-from-iron-titan-and-steel-20220602.html (last visited Oct. 4, 2025).

[59] *See* Rubens Moura de Carvalho, Helena Coelho Inácio & Rui Pedro Marques, *Stablecoin: A Story of (In)Stabilities and Co-Movements Written through Wavelet*, 18 Journal of Risk and Financial Management (2025).

[60] Kanis Saengchote & Krislert Samphantharak, *Digital Money Creation and Algorithmic Stablecoin Run*, 64 Financial Reseatch Letters, Article 105435 (2024).

[61] Financial Stability Oversight Council, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc (last visited Oct. 6, 2025).

Transparency Act of 2022,[62] which has not yet been written into law provides a comprehensive guide to ensure the full backing of stablecoins. State regulatory bodies like the New York Department of Financial Services (hereinafter NYDFS) have also imposed regulations on stablecoin bases.[63]

The FSOC, whilst not having proposed a regulatory framework, has made recommendations pertaining to stablecoin legislation. In particular, its 2021 Annual Report referenced another report by the President's Working Group on Financial Markets, which suggested that stablecoin issuers should be subject to "prudential regulatory standards", and that only "insured depository institutions" should be allowed to issue stablecoins.[64] Such recommendations would allow for more stringent capital reserve requirements, but would also require stablecoin issuers to obtain a banking charter and meet far more rigorous banking regulations. These recommendations go against the spirit of cryptocurrencies. Adopting them would compromise the privacy that cryptocurrencies offer, and further subject cryptocurrencies to the same regulations they were created to avoid.

In any case, the Stablecoin Transparency Act of 2022 provides a more promising alternative: the bill requires stablecoin bases to "publish monthly reports on their reserves", where said reports are required to be "audited by a third party".[65] This allows regulatory bodies to verify that stablecoin bases maintain fully-backed reserves, whilst ensuring minimal disruption to their operations.

Lastly, the NYDFS's virtual currency regulations provide a similar framework to the Stablecoin Transparency Act: Section 200.14 of the regulations mandates that entities engaged in virtual currency activities including stablecoin issuers must "*disclose their financial statements*" following the close of the fiscal quarter.[66] This would, in turn, include the disclosure of their reserves.

In the UK, stablecoins issued as e-money are to be fully backed by reserves, as delineated by the 2011 Electronic Money Regulations (hereinafter EMR). In this case, the FCA is the governing body for stablecoin issuers, and has applied the EMR to its corresponding set of guidelines.[67]

---

[62] *See* H.R.7328 (2021-2022). Available at: https://www.congress.gov/bill/117th-congress/house-bill/7328 (last visited Sep. 23, 2025).

[63] Virtual Currency Business Licensing (2025), https://www.dfs.ny.gov/virtual_currency_businesses (last visited Oct. 12, 2025).

[64] President's Working Group on Financial Markets, Report on Stablecoins 2 (2021). Available at: https://home.treasury.gov/news/press-releases/jy0454 (last visited Jul. 12, 2025).

[65] S.3970, 117th Cong. (2023).

[66] Virtual Currency Business Licensing (2025), https://www.dfs.ny.gov/virtual_currency_businesses (last visited Jan. 5, 2025).

[67] *See* Financial Conduct Authority, Payment Services and Electronic Money – Our Approach (2024). Available at: https://www.fca.org.uk/publication/finalised-guidance/fca-approach-

Section 20 of the EMR states that electronic money institutions must "*safeguard funds that have been received in exchange for electronic money that has been issued*".[68] Accordingly, any cryptocurrency base that issues stablecoins as e-money would meet the requirement of being an "electronic money institution", and would be required to hold the funds that investors use to buy stablecoins in reserve. This ensures a system of fully collateralised stablecoins, as cryptocurrency platforms would be prohibited from using funds received as payment for any transactional purpose.

However, the phrasing of this clause of the EMR leaves it open to a loophole: under Section 20 of the EMR, a stablecoin company would not be prohibited from minting new tokens without sufficient reserves. Following Griffin and Shams' model of Tether being supply-driven,[69] a cryptocurrency company could hypothetically issue new stablecoins even without any demand for them. Merely mandating the safeguard of funds that have been received in exchange for stablecoins that have been issued does not address this problem, since there would be no funds to safeguard. Evidently, this necessitates a more precise formulation of the EMR to preclude cryptocurrency platforms from engaging in such activities. A revision of the EMR would also act as an ancillary solution to the gaps in UK legislation governing market manipulation.

Nonetheless, it is patently obvious that the scope of the EMR only allows it to address stablecoins being issued as e-money[70]. Any stablecoin not issued on the receipt of funds (for instance, a stablecoin issued as part of a system without fiat backing) would thus fall outside of the regulatory requirements of the EMR, creating opportunities for exploitation.

More broadly, stablecoins are regulated by the 2021 Financial Services Act, which was introduced as a refinement of the FSMA. As detailed by Sections 22-24 of the Act, stablecoin companies are required to meet prudential standards, including capital requirements: a company's regulatory capital should be "*of sufficient quality to absorb losses when required*", such that it would be able to resume operations even during massive price drops.[71] In particular, the Investment Firms Prudential Regime (hereinafter IFPR) provides a comprehensive benchmark for the quality of regulatory capital which can be used as a reference.

payment-services-electronic-money-2017-november-2024-tracked-changes.pdf (last visited Oct. 12, 2025).

[68] The Electronic Money Regulations, Regulation 20 (2011). Available at: https://www.legislation.gov.uk/uksi/2011/99/regulation/20 (last visited Jan. 21, 2025).

[69] Griffin & Shams, *supra* note 30.

[70] Financial Conduct Authority, DP23/4: Regulating Cryptoassets – Phase 1: Stablecoins (2023), https://www.fca.org.uk/publication/discussion/dp23-4.pdf

[71] *National Security and Investment Act 2021,* c. 25, s. 22-24. Available at: https://www.legislation.gov.uk/ukpga/2021/25/section/22 (last visited Aug. 25, 2025).

Overall, the largest flaw in both the US and UK's legislation is the broadness of their regulations, which do not directly address the specific risks of stablecoins. One cardinal issue is the lack of any distinction between fiat-backed and algorithmic stablecoins, which results in a failure to acknowledge the comparatively higher risks of algorithmic stablecoins. Whilst some regulations allow for a more stable market structure, they completely disregard the category of algorithmic stablecoins, which rely on algorithms rather than reserves to maintain their peg. Thus far, no security mandates have been placed on the algorithms governing these stablecoins, making them susceptible to massive price fluctuations. This same insufficiency is similarly present in the legislation of all six jurisdictions discussed in this paper.

In the EU, the MiCAR governs reserve backing of stablecoin companies under 4 key provisions: the reserve of assets, auditing and transparency, redemption rights, and risk management. Stablecoins classified as e-money can be further regulated under the Electronic Money Directive (hereinafter EMD).

This part will address each of the 4 provisions of MiCAR in turn. Articles 30 and 36 of MiCAR mandate a firm to maintain a reserve of assets at all times via the disclosure of "*the amount of asset-referenced tokens in circulation, and the value and composition of the reserve of assets [on an accessible place on a company's website*".[72] Prior to this disclosure, a stablecoin company is required to undergo an independent audit by a third party, which is similarly specified under Article 30 of MiCAR. These two requirements necessitate greater transparency in stablecoin firms, and prevent the forgery of false documents regarding a firm's assets in reserve. Additionally, article 36 of MiCAR provides for risk management protocols, whereby issuers of asset-referenced tokens (i.e. stablecoins) must have a "*clear and detailed policy describing the stabilisation mechanism of such tokens*".[73] Nonetheless, no particular stabilisation mechanism is suggested, which likely implies that the regulation has no restrictions on riskier stabilization mechanisms such as algorithmic mechanisms.

Compared with other legislative frameworks, MiCAR better encompasses all categories of stablecoins in that it can be extended to algorithmic stablecoins. However, as mentioned above, it does not explicitly make mention of algorithmic stablecoins, and thus lacks a more stringent framework to govern the heightened risks of algorithmic stablecoins. This presents a potential avenue of exploration in subsequent refinements of the framework.

Other than MiCAR, the EMD regulates stablecoins classified as e-money. As Clause 11 of the Directive indicates, cryptocurrency companies are

[72] *Supra* note 47.

[73] *Ibid.*

required to enact a regime for initial capital as well as ongoing capital to ensure sufficient consumer protection and prudent operations, as well as impose an "additional method for calculating ongoing capital".[74] This additional method should be specific to a firm's properties, and can be used to ensure that the reserves required by a firm match the firm's risk levels. Moreover, the Directive further requires a company to keep the funds of e-money holders separate from the funds of its business activities, which, at its core, functions as a reserve requirement. Nonetheless, this regulation only applies to stablecoins classified as e-money and is thus limited in its scope.

To address the threat of partially backed reserves, France adopts the EU's MiCA Regulation in addition to enacting domestic legislation like the Plan d'Action pour la Croissance et la Transformation des Entreprises (hereinafter PACTE) Law.

National French laws governing stablecoins generally take reference from the MiCA Regulation, which has four key requirements: maintaining a full reserve of assets, ensuring transparency through audits, accommodating customers' redemption rights, and risk management.

As for the PACTE Law, it addresses the issuance of digital assets and indirectly mandates the proper maintenance of reserves. Under Section I(b) Article L. 524-3, payment institutions are required to provide proof of a paid-up capital or guarantee from a credit institution or finance company for an amount minimally equal to the sum set by the Minister of Finance.[75] Both of the above requirements act as a financial safety net for stablecoin companies, as they will ensure that a company has sufficient reserves to back the amount of stablecoins in circulation. To exemplify, in the event that a company fails to meet its obligations, a guarantee allows the company to rely on the guaranteeing entity to cover the outstanding amount. Whilst capital requirements and guarantees are not considered reserves per se, they can still address the issue of partially backed stablecoins by contributing to a company's liquid assets. This provides greater financial stability for a company, preventing it from becoming insolvent in the event of a mass redemption of stablecoins.

Nonetheless, this article does not address a company's maintenance of reserves as it primarily applies to companies seeking registration for those already registered under the AMF, there are no further requirements on the disclosure of internal activities. In light of this, one potential approach to consider would be implementing an annual audit report focused specifically

[74] Directive 2009/110/EC of the European Parliament and of the Council, (11) (2009). Available at: https://eur-lex.europa.eu/eli/dir/2009/110/oj/eng (last visited May 2, 2025).

[75] LOI n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises [Law No. 2019-486 of May 22, 2019, on the Growth and Transformation of Companies], 524 § 3. Available at: https://www.wipo.int/wipolex/en/legislation/details/19872 (last visited Sep. 12, 2025).

on a company's reserves, which would be a more efficacious way of ensuring consistent transparency.

Additionally, while there are no Kenya-based stablecoin companies as of now, regulations should still be in place to monitor the full backing of reserves for stablecoin companies established overseas. However, Kenya currently has no regulations in place to govern the full backing of a stablecoin platform's reserves. Such a problem would not pose too much of an issue if Kenyan laws on transparency and audit requirements could be extended to apply to cryptocurrencies; however, even among traditional markets, audit and disclosure requirements are sparse.

Section 29 of the Capital Markets Act on Licensing Agreements only requires that applicants have, inter alia, administrative capabilities and the ability to continue their business under various circumstances.[76] Compared to the licensing requirements in other jurisdictions, this section notably lacks a clause on audit requirements. Hence, stablecoin platforms used in Kenya might not be required to disclose the proportion of funds they hold, at least within Kenya. This opens up the possibility of a cryptocurrency platform establishing a subsidiary in Kenya to unlawfully mint new tokens, a practice that might go unnoticed for an extended period of time.

Under this scenario, there nonetheless exists a saving grace for Kenya. Since the governments of other developed countries would have established more robust frameworks to govern the full backing of stablecoins, stablecoin companies operating primarily within those jurisdictions would be subject to comprehensive regulatory oversight. By extension, any subsidiaries of these companies operating in Kenya would likely remain under the purview of other jurisdictions, making up for the insufficiencies in Kenya's legal frameworks.

Finally, in Singapore, the MAS's Payment Services Act (PSA) governs all forms of payment services, including that of stablecoins.[77] Its licensing requirements thus address stablecoin companies, while complementary guidance is provided by its Consultation Paper on Stablecoins.

As Section 16 of the PSA stipulates, an authority may require a licensee to provide information relating to its operations,[78] which would likely include details on the stablecoins in circulation and their reserves. This would provide a point of regulation for authorities to ensure that a company's stablecoins are fully backed by reserves authorities would be able to obtain information even in the absence of concrete proof, thereby creating a more transparent system. Moreover, Section 17 of the Act requires licensees to submit reports that cover

[76] *Supra* note 52, Section 29.

[77] *See* Monetary Authority of Singapore, Payment Services Act (2019). Available at: https://www.mas.gov.sg/regulation/acts/payment-services-act (last visited Oct. 12, 2025).

[78] *Id.*, Section 16.

details specified by an Authority[79]. In the case of stablecoin companies, an Authority would likely impose more stringent requirements for the contents of the report, which might include a breakdown of a company's reserves. In this respect, the PSA provides a more robust framework than some of the other jurisdictions discussed in this paper, as it allows for ongoing monitoring of a company's reserves rather than a singular check at the time of registration.

Additionally, Section 4.21 of the MAS's 2022 Consultation Paper on Stablecoins indirectly addresses the maintenance of reserves: a company must hold, at all times, liquid assets which are "*valued at the higher of 50% of annual operating expenses or an amount assessed by the [stablecoin] issuer to be needed to achieve recovery or an orderly wind-down*".[80] Furthermore, the company is prohibited from engaging in additional business practices that could introduce new risks, a restriction likely suggested in view of the inherent risks already associated with stablecoins. Though these clauses do not directly relate to the backing of stablecoins, they allow a company to have sufficient reserves to remain solvent in the case of massive sell-offs. It should further be noted that they have not yet been written into law, but nonetheless provide a good regulatory framework to account for financial downturns.

Even so, there is room for improvement in both the existing legislation and the suggestions made in the Consultation Paper. Specifically, it would be prudent to mandate that companies compile third party audit reports on their reserves. If filed annually, these audit reports would provide a solid foundation for monitoring, and directly address the risks associated with partially backed stablecoin reserves.

C. Recommendations for a Global Legal Framework

Overall, the US's Stablecoin Transparency Act provides the most comprehensive framework in addressing the full backing of stablecoins. Specifically, its mandate for stablecoin firms to publish monthly reports on their reserves, as audited by a third party, enables maximum transparency in a firm's operations. By cross-referencing a firm's reserves against the number of stablecoins it has in circulation, regulatory bodies can easily identify firms that only back up their stablecoins partially. Similarly, the NYDFS mandates stablecoin issuers to disclose their financial statements. In doing so, regulatory bodies can assess the equity section of a firm's balance sheet, which typically provides information about a company's reserves. Since the US's legal frameworks generally offer the most bespoke approach to stablecoin backing,

[79] *Id.*, Section 17.

[80] Monetary Authority of Singapore, Consultation Paper on Proposed Regulatory Approach for Stablecoin-Related Activities , Section 4.21 (2022). Available at: https://www.mas.gov.sg/publications/consultations/2022/consultation-paper-on-proposed-regulatory-approach-for-stablecoin-related-activities (last visited Oct. 12, 2025).

(1) *its frameworks should be referenced in the development of a global legislative framework*.

By contrast, the other jurisdictions discussed in this paper either lack this clause entirely, or only require audit reports during registration. This is evidenced in the UK's EMR and the EU's MiCA Regulation, both of which are only applicable to stablecoin firms at the time of their registration under a suitable regulatory body. While these regulations can also be used as a reference, it is important to note that modifications must be made to include consistent periodic audits. These audits would allow consistent monitoring of a company's reserve pool, minimising the occurrence of illicit activities during periods where regulatory oversight is limited.

One other clause that is worthy to note is that of Singapore's MAS Consultation Paper on Stablecoins, which prohibits companies from engaging in additional business practices that could introduce new risks. Given the inherent risks that are already associated with stablecoins, this clause allows for a step-by-step approach to risk mitigation. That is, since the partial backing of stablecoins currently presents a significant threat, this framework should be employed until the threat is better understood. Perhaps counterintuitively, this clause is crucial to the long-term progress of stablecoin firms: failing to address the risks of partial reserves can lead to insolvency, while robust internal controls are necessary to provide a solid foundation to innovate further. Hence, **(2)** *this clause should be taken into consideration for the global legal framework—at least until the risks of stablecoins are better understood and the framework proves effective in minimising the risks of partially backed stablecoins*.

Lastly and perhaps most importantly, it should be noted that none of the legislative frameworks discussed in this paper include a specific clause on algorithmic stablecoins. To exemplify, algorithmic stablecoins are currently unregulated under the MiCA Regulation, meaning that any issues regarding the price of a platform's algorithmic stablecoins may be surfaced too late. Additionally, the FSA's legal framework offers an exhaustive regulatory safeguard against the threat of partially backed reserves, but would nevertheless benefit from minor tweaks. Most notably, the IFPR's benchmarks are largely designed for investment firms holding a larger proportion of traditional assets.[81] Stablecoins, being a more volatile asset class,[82] would thus need more stringent regulatory standards, potentially in the form of a separate clause specifically addressing stablecoins. As Clements aptly puts it, if a product requires a minimum level of demand to function, as in the case of

[81] Investment Firms Prudential Regime (IFPR) (2021), https://www.fca.org.uk/firms/investment-firms-prudential-regime-ifpr (last visited May 7, 2025).

[82] Hossein Nabilou & André Prüm, *Central Banks and Regulation of Cryptocurrencies, 14 Review of Banking and Financial Law*, 27 (Working Paper No. 2019-014, 2019).

stablecoins, it is inherently fragile.[83] Therefore, leaving algorithmic stablecoins without regulation or, at least, without enforceable regulations is a recipe for insolvency. Krause further delineates three other risks of algorithmic stablecoins: (1) death spirals, where a stablecoin's unpegging leads into a cascade of sell-offs; (2) speculative attacks, where periods of mass redemption can undermine a stablecoin's peg; and (3) trust and transparency risks, where a perceived weakness in the algorithm can lead to panic and large-scale sell-offs.[84]

Evidently, algorithmic stablecoins present more amplified risks than their fiat-backed counterparts, and it is thus imperative for algorithmic stablecoin platforms to comply with more stringent regulations.

Accordingly, **(3)** *the global legal framework should only allow the operation of algorithmic stablecoin platforms with cybersecurity systems capable of adhering to its standards*. Platforms lacking these systems should not be permitted to continue operations until a system is implemented, or until an effective way to mitigate the heightened risks of algorithmic stablecoins is found. While this may seem like an excessively rigorous measure, it is necessary given the significant risks of algorithmic stablecoins, which cannot be directly addressed by legislation due to the difficulty of enforcement.

In summary, the regulatory proposals to address the backing of stablecoins are as follows: first, stablecoin firms should be mandated to publish annual audit reports on their reserves, in order to ensure that 1:1 backing is in place. Stablecoin companies should also be prohibited from engaging in additional business practices that could introduce new risks due to the high volatility of stablecoins. Finally, only platforms that have sufficiently robust cybersecurity systems should be allowed to operate in order to prevent criminal activity on such platforms.

VI. Money Laundering (ML) and Terrorism Financing (TF)

A. Overview of Risk

Due to its pseudonymous nature and relative separation from government intervention, the cryptocurrency cybersphere is a prime breeding ground for money laundering and terrorism financing activities. In recent years, decentralised exchanges (DEXs) have gained attention for their ability to bypass Know Your Customer (KYC) and Anti-Money Laundering (AML)

[83] Ryan Clements, *Built to Fail: The Inherent Fragility of Algorithmic Stablecoins,* 11 Wake Forest Law Review 131, 139 (2021).

[84] David Krause, *Algorithmic Stablecoins: Mechanisms, Risks, and Lessons from the Fall of TerraUSD*, 9 (2025). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5092827SSRN (last visited Aug. 6, 2025).

regulations.[85] As cryptocurrency exchanges that allow peer-to-peer trades without a central body to facilitate the transfer of funds, DEXs are in a far more volatile position than their centralised counterparts—CEXs, or centralised exchanges[86]. It should be noted here that "decentralised" and "centralised" refer to how the DEX and CEX platforms themselves operate, although the blockchain technology used in both is decentralised, in that it is not governed by a single entity.

From a regulatory perspective, CEXs are much easier to regulate via AML/KYC legislation, as regulatory tasks can be assigned to the organisation managing the platform. DEXs, however, lack a controlling body, rendering it difficult for legislators to find a point of accountability. In this regard, criminals are incentivised to utilise DEXs as platforms to liquidate stolen assets.

Even so, while DEXs require more stringent regulations than CEXs, both present the same foundational risks pertaining to ML and TF. A scandal involving a cryptocurrency platform facilitating ML/TF could lead to investors losing trust in the platform, causing the platform's tokens to suffer massive price drops. Although ML and TF activities are far more likely to result in losses in revenue rather than complete insolvency, they can just as easily play a secondary role to other contributing factors in a platform's insolvency.

In the Tornado Cash sanctions case, as previously discussed in the introduction, the US Office of Foreign Assets Control (OFAC) imposed sanctions on Tornado Cash, a privacy-enhancing protocol on the Ethereum blockchain. Since its establishment in 2019, the protocol has expedited the transfer of over $9B USD in funds to terrorist groups like the North Korean government-run hacker group Lazarus Group, as well as for use in other illicit activities.[87] The OFAC's subsequent sanctions prevented American citizens from using the protocol, effectively barring it as an avenue for ML/TF activities. As delineated by software company TRM Labs Inc., the volume of transactions on Tornado Cash dropped steeply after it was sanctioned,[88] corroborating the claim that a platform's facilitation of ML/TF activities can engender a loss of trust in said platform.

---

[85] Angelo Aspris et al., Decentralized Exchanges: The "Wild West" of Cryptocurrency Trading, 77 International Review of Financial Analysis, Article 101845 (2021).

[86] CEX vs DEX: The Complete Guide to Crypto Exchanges (2024), https://share.google/QrjL3Jq7gRCT3bdkf (last visited Oct. 6, 2025).

[87] Press Release, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (2022). Available at: https://home.treasury.gov/news/press-releases/jy0916 (last visited Sep. 21, 2025).

[88] Tornado Cash Volume Dramatically Reduced Post Sanctions, But Illicit Actors are Still Using the Mixer (2023), https://www.trmlabs.com/resources/blog/tornado-cash-volume-dramatically-reduced-post-sanctions-but-illicit-actors-are-still-using-the-mixer (last visited Oct. 6, 2025).

However, even with this victory against the threat of ML and TF, the cryptospace is still vulnerable to an evolving version of the threat. As Takei observes, the techniques used to evade blockchain analysis have shifted as a result of the Tornado Cash sanctions, meaning that legislators have to stay vigilant in order to enact legislation in accordance with evolving criminal techniques.[89]

B. Cross-Jurisdictional Analysis

In the United States, the international standards set by the Financial Action Task Force (FATF)[90] are adhered to, in addition to domestic regulations like the Financial Crimes Enforcement Network (FinCEN)[91] and the USA Patriot Act.[92] I note that the FATF guidelines are adhered to by all six jurisdictions discussed in this paper.

To begin, the FinCEN's Bank Secrecy Act (BSA) requires cryptocurrency exchanges to comply with KYC policies.[93] Section 8.1 of the Act mandates the collection of customer identifying information when a customer opens a cryptocurrency account[94]; this information will then be disclosed to FinCEN, allowing for the identification of individuals associated with ML activities, or individuals associated with terrorist groups. This might seem counterintuitive to the pseudonymous nature of cryptocurrency systems, but in actuality, it is *transactions* which remain pseudonymous, not *investors themselves*. Such a framework thus allows for the identification of individuals who are likely to engage in illicit activity.

Subsequently, cryptocurrency bases will be required to freeze assets related to terrorist organisations/ML activities, as governed by the USA Patriot Act.[95] This allows the transfer of funds to terrorist organisations to be blocked, and also prevents the proceeds of illicit activities from being reintroduced into the financial system under the guise of legitimacy.

---

[89] *See* Yuto Takei & Kazuyuki Shudo, *FATF Travel Rule's Technical Challenges and Solution Taxonomy*, IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 784 (2024).

[90] Virtual Assets (2023), https://www.fatf-gafi.org/en/topics/virtual-assets.html (last visited Oct. 5, 2025).

[91] FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing (2023), https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency (last visited Oct. 5, 2025).

[92] David Stier & Eric Hall, Treasury proposes designating transactions with cryptocurrency mixers a "Primary Money Laundering Concern" (2023), https://www.dlapiper.com/en/insights/publications/2023/10/treasury-proposes-designating-transactions-with-cryptocurrency-mixers (last visited Oct. 4, 2025).

[93] 31 U.S.C. § 5311.

[94] The Bank Secrecy Act, Section 8.1 (1970). Available at: https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act (last visited Oct. 11, 2025).

[95] 50 U.S.C. § 1801.

The FATF recommends a similar framework that can be implemented in 3 sections: customer due diligence (CDD) and record keeping, additional measures for specific customers, and reporting of suspicious transactions.[96] Customer due diligence involves the collection of customer identifying information as delineated in the FATF's Travel Rule[97], while documents containing such information are typically mandated to be kept for 5 years.[98]

Moreover, customers who may present higher risks are subject to additional security measures: for instance, politically exposed persons (PEPs), who are defined as individuals entrusted with a prominent function by an international organisation,[99] are required to go through enhanced CDD measures owing to their susceptibility to bribery or corruption. Finally, suspicious transaction reports are filed by exchanges when a potentially illicit transaction is identified: though transactions on the blockchain are pseudonymous, they are still traceable via blockchain analysis tools.[100]

Similarly, the threats of money laundering (ML) and terrorism financing (TF) in the cryptosphere are addressed by the UK Proceeds of Crime Act (POCA), the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations, the Terrorism Act, and the international Financial Action Task Force (FATF) regulations. As with most other financial regulations in the UK, the enforcement of these acts falls under the jurisdiction of the UK Financial Conduct Authority (FCA).

To begin, POCA criminalises ML and similarly creates offences for the failure to report a suspicious transaction/suspicion of ML Under the Act, any individual in a regulated sector (in this case, an employee of the cryptocurrency base) who suspects another person of engaging in ML activities is required to report their suspicion to an appointed officer. The appointed officer will then file a Suspicious Actions Report (SAR) to the National Crime Agency (NCA), whereupon the failure to do so will result in a "sentence of up to 5 years and an unlimited fine".[101] Section 18(1) of the

[96] *See* International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (2012). Available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (last visited Sep. 21, 2025).

[97] *See* FATF updates Standards on Recommendation 16 on Payment Transparency (2025). Available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html (last visited Sep. 21, 2025).

[98] 31 C.F.R. § 1010.410(e) (1972).

[99] LexisNexis Risk Solutions, What is a Politically Exposed Person (PEP) (2021), https://risk.lexisnexis.com/global/en/insights-resources/article/what-is-a-politically-exposed-person (last visited Oct. 15, 2025).

[100] *See* Anastasios Balaskas & Virginia N. L. Franqueira, *Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges*, 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (2018).

[101] Proceeds of Crime Act, Section 29 (2002). Available at: https://www.legislation.gov.uk/ukpga/2002/29/section/29 (last visited Aug. 3, 2025).

Terrorism Act similarly penalises any individual who fails to report their suspicion despite reasonable cause to suspect another person of engaging in TF activities.[102]

Moreover, companies are required to comply with CDD measures under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations, which were established to complement POCA. The regulation includes a specific clause for cryptoasset exchange providers, mandating the collection and record of customer information "in relation to a cryptoasset transfer which is equal to or exceeds the equivalent in cryptoassets of 1,000 euros in value".[103] Since perpetrators engaging in illicit ML activities typically transfer large funds into cryptocurrency exchanges, verifying personal data when a user exceeds the €1,000 threshold allows for the identification of suspicious persons (such as through the cross-referencing of personal data against sanctions lists).

Other than the aforementioned acts, the FATF regulations also govern ML and TF activities in the UK.

In the EU, the main legal framework regulating money laundering (ML)/terrorism financing (TF) activities is the 6th Anti-Money Laundering Directive (AMLD6)[104]. The directive, which was introduced as a refinement of the 5th Anti-Money Laundering Directive (AMLD5)[105], applies to 'obligated entities', the definition of which was expanded to include CASPs.

In particular, the Directive mandates that EU operators implement adequate measures to deal with EU sanctions risks through, *inter alia*, implementing internal policies and controls, risk assessment protocols, and updated CDD measures. Other than imposing similar rules to the FATF's international recommendations, AMLD6 introduces new circumstances where CDD measures are necessitated[106]. Occasional transactions that do not constitute a business relation, for instance, are required to be monitored through the use of CDD measures if they exceed the threshold of €10,000, a lower threshold than the €15,000 minimum originally proposed by AMLD5.[107]

---

[102] Terrorism Act, § 18(1) (2000). Available at: https://www.legislation.gov.uk/ukpga/2000/11/contents (last visited Aug. 16, 2025).

[103] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations, § 27 (2017). Available at: https://www.legislation.gov.uk/uksi/2017/692/contents (last visited Aug. 16, 2025).

[104] *See* Directive 2018/843 of the European Parliament and of the Council (2018). Available at: https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng (last visited Aug. 16, 2025).

[105] *See* Directive 2015/849 of the European Parliament and of the Council (2015). Available at: https://eur-lex.europa.eu/eli/dir/2015/849/oj/eng (last visited Aug. 16, 2025).

[106] Melvin Tjon Akon et al., The New Anti-Money Laundering Rules: What You Need to Know, https://www.dlapiper.com/en/insights/publications/2024/12/the-new-anti-money-laundering-rules-what-you-need-to-know (last visited Oct. 15, 2025).

[107] *See* Council Directive 2021/514 (2021). Available at: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32021L0514 (last visited Aug. 17, 2025).

Specific CDD requirements are also mandated for cross-border correspondent relationships, owing to the high risk associated with cases of cross-border ML and TF activities[108]. Furthermore, in the event that an individual reasonably suspects another person of engaging in a suspicious transaction, an SAR must be filed to a local Financial Intelligence Unit (FIU), as per standard practice[109].

A complementary framework to the AMLD6 is the EU Regulation on Information Accompanying Transfers of Funds, which lays down a directive on the collection of information of payers or payees in a transaction. Clause 9 of the Regulation mandates full traceability of the transfer of funds,[110] requiring the collection of information regarding payees and payers to accompany the transaction. Though transactions are pseudonymous (the public address of users on cryptocurrency platforms is not linked to their personal identity), cryptocurrency firms can nonetheless verify users' identities through the information collected from the KYC process at the time of account registration.

Key pieces of legislation governing the threat of ML/TF in France include the EU's AMLD6, the Ministry of Finance's directives on Reporting Activity, and the PACTE Law. The enforcement of these laws falls under the jurisdiction of the AMF and ACPR, both of which ensure that firms maintain effective internal controls and report suspicious transactions in line with the FATF guidelines.

The EU's AMLD6 takes reference from the FATF's guidelines, and is generally applied in three clauses: customer due diligence (CDD) measures, risk assessment protocols, and internal control frameworks.

Next, France's Ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique (Ministry of Finance) issued a directive on reporting activity in 2022, underscoring the importance of more stringent due diligence measures. The report emphasised the importance of identifying transactions related to sanctioned entities, as well as improving the quality of suspicious transaction reports (STRs)—in particular, the report cited that "*certain STRs [were] not written entirely in French and [were] therefore regarded as inadmissible*".[111] Furthermore, it tentatively proposed a way of increasing reporting activity: by mandating an STR if an entity's request to enter into a business relationship was rejected on KYC grounds. This provides a

[108] Akon et al., *supra* note 106.

[109] *See* Freshfields Bruckhaus Deringer LLP, The European AML Package – A Navigator (2024). Available at: https://www.freshfields.com/globalassets/noindex/documents/the-european-aml-package-a-navigator.pdf (last visited Oct. 7, 2025).

[110] Regulation 2015/847 of the European Parliament and of the Council, (9) (2015). Available at: https://eur-lex.europa.eu/eli/reg/2015/847/oj/eng (last visited Aug. 18, 2025).

[111] *See* Ministere de l'Economie, des Finances et de la Souveraineté Industrielle et Numerique (Ministry of the Economy, Finance and Industrial and Digital Sovereignty), AML/CFT: Reporting Entities Activity (2022). Available at: https://www.economie.gouv.fr/files/2023-06/TRACFIN_2022_EN_Web.pdf (last visited May 7, 2025).

comprehensive framework to increase regulatory activity and reduce cases of ML and TF, by outlining specific requirements for businesses to follow.

However, regarding the requirement of filing STRs entirely in French, a more pragmatic approach may be warranted international firms based in France might not have French-speaking compliance officers, thus a mandate that STRs be filed solely in French could present logistical challenges. Regulatory bodies should instead utilise translation tools to accommodate STRs filed in a foreign language, allowing for the more expedient filing of STRs.

Finally, the 2020 order published by the French government in accordance with the PACTE Law targeted the implementation of more robust asset-freezing measures. The order stipulated that asset-freezing measures can be taken immediately upon confirmation that an individual is on an international sanctions list,[112] allowing regulatory bodies to swiftly prevent illicit activities like terrorism financing.

In Kenya, the Proceeds of Crime and Anti-Money Laundering Act (POCAMLA) has been extended to Virtual Asset Service Providers (VASPs) in the cryptosphere. Though the Kenyan government has no legislation specifically targeted at AML/CFT in the context of cryptocurrencies, section 2 of the POCAMLA defines property as "tangible or intangible".[113]

This provides an opening for cryptocurrencies to be classified as property and thus become subject to the same regulatory requirements as traditional firms. Kenya also tries to align itself with the FATF's requirements, though not much progress has been made in this regard.

As mentioned earlier, virtual assets like cryptocurrencies may be considered property and governed under the POCAMLA. However, the question of how they will be governed remains unanswered. In particular, although cryptocurrencies themselves may be governed under the Act, the Act does not recognise VASPs as reporting institutions.[114] This undermines the efforts of other legislation: the Companies Act, for instance, requires a company to disclose beneficial owner (an individual who owns a legal entity) details,[115] but Kenya has not appointed any governmental authority to oversee

[112] Asset Freezing: Reinforcement of the System by Order (2020), https://www.amf-france.org/en/news-publications/news/asset-freezing-reinforcement-system-order (last visited Oct. 15, 2025).

[113] The Proceeds of Crime and Anti-Money Laundering Act, Part I (2009). Available at: https://www.frc.go.ke/wp-content/uploads/2024/02/Proceeds-of-Crime-and-Anti-Money-Laundering-Act-No-9-of-2009-Revised-2022.pdf (last visited Aug. 21, 2025).

[114] Financial Reporting Centre – Kenya, Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) Money Laundering and Terrorism Financing Risk Assessment Report 66 (2023). Available at: https://www.frc.go.ke/wp-content/uploads/2024/02/VAs-and-VASPs-ML_TF-Risk-Assessment-Report-1.pdf (last visited Oct. 3, 2025).

[115] See The Companies Act (2024). Available at: https://new.kenyalaw.org/akn/ke/act/2015/17/eng@2024-12-27 (last visited Aug. 21, 2025).

such disclosure. As such, any information collected by VASPs cannot be utilised to detect illicit activities, decreasing the transparency of transactions. This nuance also allows cryptocurrency companies to bypass CDD measures, making it more difficult to detect ML and TF activities. It is evident, then, that the provisions of the POCAMLA should be extended to VASPs rather than merely virtual assets. Such an adaptation will further allow Kenyan laws to better align with the FATF standards: currently, FATF Recommendations 10 and 15 require VASPs to undertake due diligence measures and identify the source of funds, which is again hindered by the above nuance.[116]

Notwithstanding these regulatory insufficiencies, it is worth mentioning that the AML/CFT efforts of Kenyan authorities have not completely been in vain. In particular, Kenya has effective frameworks in place to obtain information related to virtual assets and VASPs from foreign jurisdictions,[117] allowing it to combat ML and TF threats posed by cryptocurrency bases established on foreign soil. Such international cooperation lessens the risk of ML and TF activities in Kenya, though it often requires a comparatively cumbersome approach which once again underscores the need for robust domestic regulations.

Finally, the Corruption, Drug Trafficking and Other Serious Crimes Act (CDSA) and the Terrorism (Suppression of Financing) Act (TSOFA) govern the threat of Money Laundering/Terrorism Financing (ML/TF) in Singapore. Both are aligned with the FATF's Recommendations, allowing for a more standardised approach to combating these threats.

Following the FATF framework, Section 43 of the CDSA mandates that financial institutions in Singapore retain transaction documents for a stipulated length of time.[118] Typically, companies are required to retain these documents for five years following the completion of a transaction, giving authorities ample time to prosecute past ML/TF activities that have come to light. Furthermore, under Section 45 of the Act, individuals with reasonable grounds to suspect another person of engaging in ML/TF activities are required to report their suspicions to a Suspicious Transaction Reporting Officer within their firm.[119] For cryptocurrency companies, employees overseeing cybersecurity would most likely uncover these threats; therefore, this Act provides a clear framework for the process of raising concerns. Beyond these stipulations, companies are also required to implement CDD measures, and carry out enhanced CDD (eCDD) checks for more high-risk

[116] Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 14, 17 (2023). Available at: https://share.google/GErnhNhbiXGKubq1v (last visited Feb. 12, 2025).
[117] *Supra* note 114, 67.
[118] The Corruption, Drug Trafficking and Other Serious Crimes Act, Section 43 (1992). Available at: https://sso.agc.gov.sg/Act/CDTOSCCBA1992 (last visited Aug. 21, 2025).
[119] *Id.*, Section 45.

individuals.[120]

In a similar vein, the TSOFA employs a framework comparable to the aforementioned Acts: under Part 4 of the Act, terrorist property may be frozen or confiscated by relevant Authorities.[121] This allows the immediate cessation of illicit activities to cut funding to terrorist organisations, demonstrating the timely intervention this Act provides for.

In general, the six jurisdictions' AML/CFT legislation, when taken with reference to the FATF framework, provides a comprehensive framework for cryptocurrency bases. However, certain types of exchanges are more elusive to these regulatory requirements. DEXs, in particular, lack a central operator or "gatekeeper" to enforce regulatory requirements such as CDD or KYC checks. As such, although agencies like the US's FinCEN have indicated that DEXs are required to undergo AML checks, it is unclear how this will be executed. Additionally, while the UK's FCA 2020 Guidance on Cryptoassets makes clear that businesses offering services like exchange and conversion must comply with AML requirements,[122] it is unclear how these requirements will be *enforced* for certain types of cryptocurrency platforms like DEXs. Whilst possible solutions have been proposed (the use of smart contracts to automate compliance, for one), they are largely still in development and are not likely to be implemented anytime soon. This provides more leeway for terrorist groups to transfer funds or launder money through DEXs, since it is difficult to obtain customer information from such platforms.

C. Recommendations for a Global Legal Framework

The legislative frameworks countering the threat of ML and TF in this paper are generally consistent with the recommendations provided by the FATF. Since most legislations generally adopt similar procedures to address this risk, the certain aspects of these procedures that should be included in the global legal framework will be delineated. Allow me to first restate the main provisions of the FATF Guidelines: a) CDD and record keeping, b) additional measures for specific customers, and c) the reporting of suspicious transactions.

These measures allow for proportionate measures to be taken in relation to the risk profile of a customer, and facilitate the expedient detection of ML and TF activities. Delving into specific jurisdictions, the US further requires firms

[120] *See* Monetary Authority of Singapore, Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services. Available at: https://www.mas.gov.sg/regulation/notices/psn01-aml-cft-notice---specified-payment-services (last visited Aug. 23, 2025).

[121] Terrorism (Suppression of Financing) Act, Part 4 (2002). Available at: https://sso.agc.gov.sg/Act/TSFA2002 (last visited Aug. 23, 2025).

[122] *See* Financial Conduct Authority, Guidance on Cryptoassets (2019). Available at: https://www.fca.org.uk/publications/policy-statements/ps19-22-guidance-cryptoassets (last visited Aug. 22, 2025).

to freeze assets related to terrorist organisations or ML activities under the US Patriot Act, which enables swift intervention against illicit activities. Moreover, the EU's AMLD6 necessitates CDD measures in new circumstances, such as occasional transactions that do not constitute a business relation. By extending the framework to cover these one-off transactions, the EU can better detect terrorism financing in the form of micro-donations, where a large group of terrorist sympathisers each make a single transaction to evade detection.[123] That is, many individuals may make small contributions that add up to a sizable sum, allowing a hefty portion of money to be raised for terrorist causes without drawing too much attention to the individual transactions. Accordingly, the aforementioned legislation should be used as reference in the development of a global framework.

Another cardinal issue that remains unaddressed in current legislative frameworks is the enforcement of legislation concerning DEXs. This issue is pertinent to most of the threats discussed, but this section will focus on it. First of all, it is essential to acknowledge the difficulty of regulating DEXs: it is not so much that current legislation does not apply to DEXs *per se*, but rather that it is far more challenging to regulate their activities. Due to their decentralised nature, DEXs lack a central organisation that may be held accountable by regulatory bodies, making it much harder for regulatory bodies to trace and target illicit activities. A pertinent example of this was the recent crackdown by Chinese authorities on the DEX HyperLiquid, which had been used as a platform for money laundering activities.[124] Due to HyperLiquid's lack of KYC requirements, money launderers could effectively post their tainted funds on the platform anonymously. By predicting that market prices would drop (opening a "short" position for their tainted funds) on a DEX, and predicting the opposite on a CEX (opening a "long" position), criminals can retrieve the cryptocurrencies lost from a DEX on a different CEX. For illustrative purposes, a criminal might open a short position sized at $5M in Bitcoin on the DEX, meaning that a decrease in market prices would result in a net profit while an increase in market prices would result in a net loss. The criminal would then open a long position sized at $5M in Bitcoin on another CEX, such that any increase in market prices on the DEX would lead to a loss of the tainted funds, simultaneously allowing the criminal to gain back "clean" money on the CEX. This illustrates the susceptibility of DEXs to illicit activities, further underscoring the difficulty of detecting such activities even with regulatory frameworks in place.

[123] *See* FATF Report, Crowdfunding for Terrorism Financing (2023). Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf (last visited Oct. 3, 2025).

[124] HyperLiquid: A New Route for Crypto Money Laundering? (2025), https://medium.com/coinmonks/hyperliquid-a-new-route-for-crypto-money-laundering-a7f1dc713d01 (last visited Oct. 4, 2025).

In response to these regulatory challenges, Guseva proposes a possible solution for the enforcement of KYC measures in DEXs:[125] the establishment of Self-Regulatory Organisations (SROs). SROs are typically supervised by regulatory bodies within a jurisdiction, and can directly gather information from market participants to approximate decentralised markets. By targeting market participants rather than exchanges themselves, SROs can circumvent the lack of a central operating body in DEXs. This approach further allows regulatory bodies to obtain user information from DEXs without the need to develop algorithms for data collection. Accordingly, I propose that DEXs that trade the same asset classes be regulated by the same SRO in order to detect instances of illicit activity across such platforms. This would make it more difficult for criminals to introduce tainted funds onto the platform, as there would be records of their activity and registration with said platform. Therefore, this approach should be a potential consideration in the development of a global legal framework.

To conclude, it is recommended that CDD measures be extended to cover instances of micro-donations, or occasional transactions that do not constitute a business relation. Additionally, SROs should be established to target market participants such that KYC and AML measures can still be carried out in the absence of a central intermediary.

VII. Theft of Cryptocurrencies

A. Overview of Risk

The final risk of cryptocurrencies is their vulnerability to theft, a threat that has frequently been overlooked by regulators who have yet to understand its full ramifications.[126] This is perhaps attributable to the isolated nature of its impact, which is generally limited to small groups of investors and individual investors. Nonetheless, as the cryptocurrency sector becomes increasingly entwined with traditional financial markets, stronger regulation will need to be imposed.

Estimates show that in the first decade since the inception of Bitcoin (2009-2019), its users have lost approximately $3.5B USD worth of Bitcoins as a result of unauthorised takings (i.e. theft).[127] Whilst some believe that the risk of theft is inherent in the use of loosely regulated cryptocurrency platforms,

[125] Yuliya Guseva, Decentralized Markets and Self-Regulation (2025), https://clsbluesky.law.columbia.edu/2025/01/31/decentralized-markets-and-self-regulation/ (last visited Oct. 15, 2025).

[126] Henry S. Zaytoun, *Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft*, 97 North Carolina Law Review 395, 400 (2019).

[127] Jim Finkle & Jeremy Wagstaff, Hackers Steal $64 Million from Cryptocurrency Firm NiceHash (2017), https://www.reuters.com/article/business/hackers-steal-64-million-from-cryptocurrency-firm-nicehash-idUSKBN1E10AQ/ (last visited Oct. 15, 2025).

others have filed complaints to regulatory agencies regarding the problem.[128] Contrary to its portrayal in these scenarios, however, theft in the cryptospace is not an issue confined solely to the individual. On a broader level, it could signify a fundamental flaw within the algorithm of a cryptocurrency platform which, if left unresolved, could be exploited to a much larger extent. In light of the substantial losses that such an exploitation would precipitate, it follows that a large-scale, organised theft would have the potential to catalyse a company's insolvency.

This underscores the importance of a more robust and bespoke security framework than is mandated by current legislative measures: most of the frameworks targeting theft in the six target jurisdictions tend to borrow from solutions designed to address other risks, as will be discussed later. This engenders an excessively broad and inadequately customised framework, thereby leaving cryptocurrency platforms vulnerable to potential security breaches.

B. Cross-Jurisdictional Analysis

In the United States, the majority of legal frameworks governing the theft of cryptocurrencies focus on pursuing and prosecuting perpetrators once a crime has been detected. For this reason, this section will not make specific mention of such legislation and will instead focus on those that provide for the detection of theft in the crypto space.

Arguably, the closest the US has come to enacting a comprehensive legal framework specifically targeting the theft of cryptocurrencies was in the NYDFS's introduction of the Virtual Currency Regulation. Section 200.16 of the regulation governs the maintenance of an effective cybersecurity program to protect "sensitive data" stored in a licensee's electronic systems specifically, the program must be designed to: (1) identify cyber risks, (2) protect a licensee's electronic systems, (3) detect any data breaches or hacks to the system, (4) respond to any of the events which might arise in (3), (5) recover from such events and resume operations.[129]

A cybersecurity policy must also be implemented by the licensee, in this case, the cryptocurrency base to address, *inter alia*, incident response.

In principle, such a framework would mandate cryptocurrency bases to implement robust cybersecurity frameworks to detect theft in real time. It is all too unfortunate, then, that the regulation does not specify any state-of-the-

[128] See Lily Katz & Julie Verhage, Bitcoin Exchange Sees Complaints Soar (2017), https://www.bloomberg.com/news/articles/2017-08-30/bitcoin-exchange-sees-complaints-soar-as-users-demand-money (last visited May 3, 2025); Jen Wieczner, Hacking Coinbase: The Great Bitcoin Bank Robbery (2017), http://fortune.com/2017/08/22/Bitcoincoinbase-hack/ (last visited May 3, 2025).

[129] New York Department of Financial Services, Virtual Currency Business Licensing, Section 200.16 (2015). Available at: https://www.dfs.ny.gov/virtual_currency_businesses (last visited Aug. 23, 2025).

art cybersecurity measures to be taken. Due to the ever-evolving tactics used by cryptocurrency thieves,[130] the broad mandate of an "effective cybersecurity program" is insufficient to address newly emerging cybersecurity threats. Instead, legislation should constantly be reviewed by regulatory bodies in order to combat such threats, via the mandate of specific measures in response to new hacking methods.

Next, under UK common law, cryptocurrencies have generally been classified as properties, a position most notably affirmed by the ruling in *AA v. Persons Unknown*.[131] In this landmark case, the Honourable Mr Justice Bryan concluded in his judgement that "cryptoassets such as Bitcoin are property", thereby establishing a crucial precedent regarding the classification of cryptocurrencies. This classification, in turn, allows for cryptocurrencies to be regulated under the 1968 Theft Act, however, given that the Act is used to prosecute rather than detect theft, it will not be discussed in detail here.

A more bespoke framework for the detection of theft would instead be the FCA's Operational Resilience Guidance, which recommends the implementation of cybersecurity measures by cryptocurrency companies. Specifically, its rules require that "[...] *by no later than 31 March 2025, firms must have performed mapping and testing so that they are able to remain within impact tolerances*",[132] indirectly mandating effective cybersecurity measures to be put into place.

However, this framework only governs cryptocurrency firms registered under the FCA's cryptoasset registration regime or firms registered as payment/e-money institutions, meaning any firms falling outside of these parameters may not be subject to the same regulatory requirements. The FCA should thus consider expanding the scope of its Operational Resilience Guidance, so as to ensure that all cryptocurrency firms are held to stringent cybersecurity standards.

Another potential issue with the FCA's Guidance is that it reflects similar gaps found in US regulatory frameworks. The lack of detailed specifications regarding security measures engenders an excessively broad framework, which may fall short in addressing emerging theft tactics within the cryptospace.

In the EU, the threat of theft in the cryptosphere is regulated under the

---

[130] Oluwatoyin Ajoke Farayola, *Revolutionising Banking Security: Integrating Artificial Intelligence, Blockchain and Business Intelligence for Enhanced Cybersecurity*, 6 Finance & Accounting Research Journal 501, 503 (2024).

[131] AA v Persons Unknown, EWHC 3556 (Comm) (2019). Available at: https://uk.practicallaw.thomsonreuters.com/D-1046175?transitionType=Default&contextData=(sc.Default) (last visited Oct. 2, 2025).

[132] *See* Financial Conduct Authority, Building Operational Resilience (2021). Available at: https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience (last visited Aug. 25, 2025).

MiCA Regulations. Though it lacks a specific provision against theft, its frameworks can broadly be applied to address the theft of cryptocurrencies.

Under these regulations, crypto-asset offerors must implement effective arrangements to safeguard the funds or other crypto-assets raised during a public offering, thereby preventing the theft of funds raised during the initial offering process. Whilst MiCAR does not recommend specific cybersecurity measures for cryptocurrency bases to adopt, it indirectly encourages cryptocurrency platforms to implement the most robust frameworks: under Article 75 of the Regulations, CASPs can be held liable to their clients for any losses as a result of an incident attributable to them.[133] As such, cryptocurrency bases will be likely to adopt enhanced security protocols to minimise the risk of being held liable for customer losses.

I note here that the phrasing of Article 75 is ambiguous in that it is unclear whether "*an incident attributable to [a CASP]*" refers to overall negligence in safeguarding protocols, rather than just a specific incident involving a temporary compromise of a company's protocols. Accordingly, a refinement of this clause would allow for a more comprehensive framework.

The most glaring problem with both of the aforementioned regulations, however, is the lack of a specific clause to address the theft of cryptocurrencies. Whilst MiCA Regulations like Chapter 2 of Title V provide for the implementation of internal regulatory structures, their primary focus is on addressing other risks to which cryptocurrency platforms are vulnerable. Therefore, there is a limit to their applicability on the issue of theft, underscoring the need for new provisions specific to this threat.

Next, under French law, cryptocurrencies can be classified as property: a 2020 decision by the Court of Nanterre was the first of its kind in characterising Bitcoin as a "consumable asset", or an asset which is "consumed" through the purchase of goods and services.[134] This landmark ruling prompted the broader classification of cryptocurrencies as fungible assets or properties, allowing them to meet the definitional standards necessary to fall under existing legislation. Consequently, cryptocurrencies have become subject to criminal prosecution in cases of theft (since theft is defined as the fraudulent taking of property belonging to another individual)[135] under the French Criminal Code.

---

[133] *Supra* note 47.

[134] Bitspread v. Paymium, Tribunal de commerce de Nanterre 2018F00466 (2020). Available at: https://www.labase-lextenso.fr/sites/lextenso/files/lextenso_upload/tribunal_de_commerce_de_nanterre_6e_ch._26_fevr._2020_n_2018f00466.pdf (last visited May 4, 2025).

[135] Pierre De Roquefeuil, Quels sont les délits les plus communs et leur répression en droit français (2023), https://roquefeuil.avocat.fr/en/violence-sexual-assault-theft-narcotics-defamation/#:~:text=Theft%3A%20Theft%20is%20the%20fraudulent,a%20fine%20of%2045%2C000%20euros (last visited May 12, 2025).

However, to address the *detection* of theft, the AMF has issued a document outlining the Cybersecurity System of Requirements for DASPs. The document addresses these requirements under a few main sections including, *inter alia*, (1) a cybersecurity program, (2) operational measures, (3) distributed ledger technology and electronic wallet security and (4) security incident reporting.[136] The first section is especially salient in its recommendation of Hygiene security measures; the ANSSI Computer Hygiene Guide, for instance, delineates 42 IT security rules which allow for protection against cyberattacks.[137] These references accordingly provide a foundation for DASPs to establish a robust cybersecurity system.

Moreover, the document stipulates that companies must implement "systems to monitor the presence and effectiveness of the security measures identified in advance", thereby enabling a proactive approach to theft prevention. By contrast, relying solely on a reactive system that responds during a theft can stymie the process of identifying perpetrators, resulting in massive losses. Cybersecurity systems that are impervious to hackers should thus serve as the first line of defence against theft, as is illustrated by this requirement.

In all, French regulations governing the theft of cryptocurrencies are commendably robust due to their explicit requirements. However, certain guidelines issued by regulatory bodies would benefit from being formalised into law, as this would more effectively reduce vulnerabilities in a company's cybersecurity system. To instantiate this, allow us to consider the earlier AMF recommendation that DASPs adopt security measures such as the HYGANSSI. While such frameworks provide good guidance for companies, the lack of a legal mandate may deter companies from implementing these measures due to the associated costs. Solidifying such frameworks into law will thus ensure more consistent adherence to strong cybersecurity practices.

In Kenya, legislation and regulations with regards to cybersecurity are significantly lacking. The Data Protection Act provides a general framework to prevent data breaches - in the cryptosphere, this may be extended to apply to cases of theft which would concurrently involve a breach of data stored within private wallets. Nonetheless, most regulatory frameworks are still in their developmental stages as Kenyan law enforcement agencies have "*inadequate [skillsets] and tools for forensic investigations on virtual asset transactions and distributed ledger technology*".[138]

I refer to Section 41 of Kenya's Data Protection Act, which requires data controllers to implement appropriate "technical and organisational

[136] *See Supra* note 49.

[137] *See* French Cybersecurity Agency, Guideline for a Healthy Information System (2020). Available at: https://cyber.gouv.fr/publications/guideline-healthy-information-system-42-measures (last visited Sep. 5, 2025).

[138] *Supra* note 114.

measures" to protect the data of their customers.[139] Though this does not apply to the theft of cryptocurrencies, any form of theft would also involve a data breach of an individual's private wallet, meaning that this framework can, *mutatis mutandis*, be adapted to counter the threat of theft.

However, it should be noted that the Act does not stipulate any specific cybersecurity measures to be taken, only that the measures are proportionate to the amount of data collected. This requirement must be modified for the purposes of combating the theft of cryptocurrencies - the implementation of state-of-the-art cybersecurity measures should be mandated as blockchain technology is susceptible to emerging cyberattack schemes. This would allow cryptocurrency platforms to have a more robust safeguard against emerging cyber threats, and could be updated regularly to incorporate new measures in response to evolving theft tactics.

Finally, Singapore's Cybersecurity Code of Practice for Critical Information Infrastructure is by far the most bespoke framework regulating how companies can combat the threat of theft in the cryptosphere. SFA, as well as the Cybersecurity Act, further governs these risks, outlining the measures that companies should take to mitigate them.

Under section 15 of the SFA, exchanges must effectively manage any risks associated with their operations,[140] including but not limited to cyberthreats. Section 17, as mentioned previously, further instantiates this requirement, stipulating that the systems involved in risk management are "*appropriate for the scale and nature of [an exchange's] operations*".[141] Though both sections provide some semblance of a guideline for companies, they are phrased vaguely and do not specify any cybersecurity measures to be taken. Since the appropriateness of a system could be subjective at least to some extent, more detailed regulations would allow for greater clarity in legal proceedings.

To address these insufficiencies, I refer to Singapore's Cybersecurity Act. Section 11 of the Act empowers the Commissioner to issue codes of practice, thereby allowing the specification of cybersecurity measures.[142] Accordingly, the most recent Code of Practice (issued in 2022) mandates a Security-by-Design framework which incorporates security into all stages of the system development program. Under Section 3.5, it also requires companies to adopt certain principles to "*reduce cybersecurity risks to the Critical Information*

[139] The Data Protection Act, Part IV (2019). Available at: https://www.kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2021/LN263_2021.pdf (last visited Sep. 25, 2025).

[140] *Supra* note 41, Section 15.

[141] *Id.*, Section 17.

[142] Cybersecurity Act, Section 11 (2018). Available at: https://sso.agc.gov.sg/Acts-Supp/9-2018/ (last visited Aug. 11, 2025).

Structure".[143] This specification provides for a more bespoke framework, eliminating ambiguity over the processes companies are required to adhere to.

Nevertheless, I note that specific cybersecurity measures are still not mandated in this Code of Practice, as that should be followed. Though these principles should be it only makes mention of principles able to provide sufficient guidance for the implementation of effective cybersecurity measures, it operates on the premise that a business will adopt these measures. By contrast, recent years have shown that especially within the cryptosphere, companies may be willing to undertake substantial risks in order to cut costs and reap profits. This is evidenced in the recent hacks of prominent cryptocurrency exchanges such as the 2020 KUCoin Hack, where over $280M USD was stolen due to lax security measures.[144] Once again, this underscores the need for more stringent frameworks to govern the threat of theft in the cryptosphere. Hence, it is imperative to mandate the adoption of specific cybersecurity measures, rather than relying on broadly framed guidelines to address this risk.

C. Recommendations for a Global Legal Framework

France's regulations once again assert their position as the most robust frameworks in governing the theft of cryptocurrencies. France's AMF document outlining the Cybersecurity System of Requirements for Digital Asset Service Providers recommends firms to adopt the ANSSI Computer Hygiene Guide, which provides a comprehensive list of IT security rules that firms can implement. This specification allows for more clarity in a firm's internal controls, preventing firms from skimping on security measures to maximise profits. However, it should be noted that the Computer Hygiene Guide is not formalised into law, and merely offers a set of recommendations for firms. This approach is subject to contention, as internal self-regulation by cryptocurrency companies or greater freedom to self-regulate has long proven ineffective. As Guseva asserts, due to negative incentives, international competition, and global price formation and arbitrage, companies are unlikely to prioritise strong security measures over profits.[138] As such, the only way to enforce stronger security measures is through legislative mandates - in this regard, it is proposed that the ANSSI Guide be incorporated into the global legal framework.

Recommendations for specific security measures are notably absent in the

[143] Cyber Security Agency of Singapore, Cybersecurity Code of Practice for Critical Information Infrastructure, Section 3.5 (2018). Available at: https://isomer-user-content.by.gov.sg/36/2df750a7-a3bc-4d77-a492-d64f0ff4db5a/CCoP---Second-Edition_Revision-One.pdf (last visited Oct. 1, 2025).

[144] Ben Charoenwong & Mario Bernardi, Decade of Cryptocurrency 'Hacks': 2011 – 2021, in The Elgar Companion to Decentralized Finance, Digital Assets, and Blockchain Technologies 147, 151 (2024).

legislative frameworks of other jurisdictions: while Singapore's Code of Practice requires companies to adopt certain cybersecurity principles, this still provides a broader framework as compared to directly specifying the cybersecurity measures a company should implement. It is even more concerning that the UK and US both lack specific recommendations for cybersecurity measures, creating ambiguity about the measures a company should implement to remain within impact tolerances.

Additionally, the EU's MiCA Regulation lacks a clause on the theft of cryptocurrencies. However, its provision regarding customer losses acts as a redeeming factor: CASPs can be held liable for any losses their customers suffer as a result of an incident attributable to them. A cybersecurity system that lacks robust algorithms would possibly qualify under this clause, incentivising cryptocurrency companies to implement more bespoke frameworks. Hence, this clause should also be considered in the development of a global framework.

In summary, the ANSSI Guide, or any relevant list of cybersecurity requirements, should be adopted by jurisdictions without such requirements. This adoption will facilitate a coordinated response to theft and ensure a more robust defence against illicit activities on cryptocurrency platforms. Additionally, in order to incentivise firms to provide more robust cybersecurity measures, CASPs should be held liable for any losses that result from inadequate systems. Such a provision gives CASPs a higher stake in protecting platform users' interests, thereby prompting them to enhance their cybersecurity systems.

VIII. Other Provisions

Before concluding, it is important to address other provisions which, while not relevant to the risks discussed earlier, are nonetheless important to our discussion. In particular, another significant area of concern regarding the development of a global legal framework is developing countries' susceptibility to exploitation. Due to their less robust legal frameworks, criminal organisations may establish firms in these countries to flout more stringent regulations that are implemented overseas. To counter this limitation, the global framework should consider (1) *requiring regulatory bodies in developed countries to a) disclose any information about possible threats or criminal organisations to developing countries. Regulatory bodies should also b) share any state-of-the-art cybersecurity measures that would be necessary in mitigating these risks, and that without which would greatly compromise the ability of developing countries to respond to threats in the cryptosphere*. Such sharing of capabilities is not antithetical to a developed state's commitment to its citizens but rather is in line with it. Sharing newly developed cybersecurity measures is not, for the most part, the act of charity that nationalist lobbyists proclaim it to be. Instead, it is the obligation of a developed nation to act in the interests of the

international order, especially when international crime, or crime in developing countries, may affect the cryptocurrency bases within the nation itself. This draws a parallel to the Common but Differentiated Responsibilities concept coined by the United Nations Framework Convention on Climate Change,[145] which acknowledges the differing capabilities of different countries in combating climate change. As an improvement from it, the proposed global framework will further attempt to address these differing capabilities, closing the gap in legislation between developed and developing countries. Furthermore, the domestic adoption of the framework in developing countries may be simplified by (2) *mandating the closure of unregistered cryptocurrency firms*. Due to the emerging area of law that governs cryptocurrencies, some firms today remain unregistered under any regulatory body. This means that such firms may be able to shirk certain reporting obligations, thereby making it more difficult to identify their illicit activities. By prohibiting the operation of unregistered firms, the burden of regulatory authorities in developing countries would be significantly reduced, particularly so in cases where resources for surveillance are limited. Any individual seeking to establish a cryptocurrency firm would thus have to bypass registration processes, making it more difficult for criminals to set up illicit platforms in developing countries. Ergo, by blocking the establishment of high-risk cryptocurrency bases entirely, the regulatory process in developing countries can be streamlined, allowing authorities to focus their resources on registered firms. It is worth noting that this framework would not completely restrict users in developing countries from trading cryptocurrencies; rather, they would still be able to access overseas cryptocurrency platforms, which would remain under the regulatory purview of overseas regulators.

However, this clause does not just extend to cryptocurrency bases in developing countries. Even in developed countries, certain firms may remain unregistered due to loopholes in legislation. Since this provides a breeding ground for illicit activities, a global framework that mandates the registration of all cryptocurrency firms under the relevant regulatory bodies will also allow for more streamlined regulation in developed countries.

Moreover, it is imperative that (3) *the global framework be updated on an annual basis*. As of 2025, the cryptocurrency market remains highly volatile, with emerging threats continuously evolving to circumvent newly implemented regulatory frameworks.[146] For a global framework to remain

[145] Common but Differentiated Responsibilities (CBDR)(2023), https://dgap.org/en/research/glossary/climate-foreign-policy/common-differentiated-responsibilities-cbdr (last visited Mar. 30, 2025).

[146] Emiliano Álvarez et al., *Comprehensive Analysis of the Crypto-Assets Market through Multivariate Analysis, Clustering, and Wavelet Decomposition,* 660 Physica A: Statistical Mechanics and its Applications, Article 130330 (2025).

effective, it must not only be enforced by a regulatory body but also be regularly refined to combat emerging risks. To ensure the enforcement and upkeep of such a framework, either an existing regulatory body, such as UNCITRAL, may be enlisted, or a global regulatory body may be created, composed of compliance officers from each participating jurisdiction. With regard to the latter, at the end of each fiscal year, the compliance officers will be required to submit a report detailing the effectiveness of their jurisdictions' implementation of the framework, along with any newly identified threats to the crypto space. These reports may be presented on an international stage, allowing for necessary adaptations to the framework which would maintain its relevance and efficacy.

Finally, I would like to address the limitations of a global framework. It is inevitable that some countries will not adopt this framework, in part due to a more cautious approach to cryptocurrencies: notably, countries like China and Saudi Arabia have placed bans on the use of cryptocurrencies.[147] Furthermore, geopolitical tensions between two countries may deter one from entering into the same framework that another is governed under.[148] For this reason, the proposed guidelines for a global framework focus only on companies that are more receptive to cryptocurrencies, as it is meant to mitigate many of the risks associated with cryptocurrencies. Admittedly, a global framework of this nature is highly stringent in certain areas, potentially reducing the level of privacy that cryptocurrencies once provided. However, given the risks inherent to cryptocurrencies, it can be contended that such measures are not only necessary but imperative without them, we would remain susceptible to a multitude of threats. Furthermore, it should be noted that the core purpose of cryptocurrencies can no longer be the maintenance of absolute privacy as evidenced in the collection of customer information for KYC and CDD measures. Rather, cryptocurrencies should be valued as a medium to expedite transactions, and a platform with relatively lower government intervention. Nevertheless, government intervention remains wholly necessary to mitigate the associated risks of cryptocurrencies, provided that the measures enacted are proportionate to the scale of the threats.

To recapitulate, in addition to the recommendations in previous sections, regulatory bodies should be required to share any state-of-the-art cybersecurity measures or disclose relevant information to developing countries. This allows for a more coordinated response to criminal activity such that developing countries are not exploited for their regulatory

[147] *See* Pwc Global Crypto Regulation Report 2023 (2022). Available at: https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf (last visited Oct. 15, 2025).

[148] Yonatan Lupu, *Why Do States Join Some Universal Treaties but Not Others? An Analysis of Treaty Commitment Preferences*, 60 Journal of Conflict Resolution 1219, 1223 (2016).

insufficiencies. Moreover, any unregistered cryptocurrency firms should be mandated to close due to their high risk profile, while the global framework should be updated annually in order to address the evolving threats within the cryptosphere.

Conclusion

In conclusion, the advent of cryptocurrencies has introduced a myriad of risks to jurisdictions across the globe, in particular: market manipulation, partially backed stablecoins, money laundering and terrorism financing, and the theft of cryptocurrencies. This paper sought to elucidate these risks and provide a comparative analysis of different jurisdictions' legal frameworks and insufficiencies. Generally, current legislation only requires slight modifications, but there are some aspects of the aforementioned risks that remain unaddressed. Notably, no legislation thus far has mandated the implementation of specific cybersecurity systems (France's Computer Hygiene Guide provides specific recommendations but has not been formalised into law). Neither have any regulations been published to address enforcement difficulties with regard to DEXs. Additionally, current legislative frameworks do not provide a standardised definition of cryptocurrencies, which complicates the legal process, especially within the context of insolvency. Finally, algorithmic stablecoins do not fall under any legislation due to their backing mechanism.

In identifying the insufficiencies of legislation in the US, UK, EU, France, Kenya and Singapore, suggestions for improvement were offered in a guideline for a global legal framework. This was aimed at expediting legal processes to better mitigate the risks of cryptocurrencies, as well as providing a more accessible framework to seek remuneration in cases of insolvency. In particular, (1) the implementation of specific cybersecurity measures should be mandated; (2) the law should cover DEXs' regulation by SROs; (3) a standardised definition of cryptocurrencies as property and commodities in all contexts, in addition to defining those that pass the Howey test as securities, should be formalised into law; (4) the framework should require algorithmic stablecoin companies that do not adhere to cybersecurity requirements to cease operations; and (5) a clause requiring developed countries to share relevant information and cybersecurity systems with developing countries should be provided. To conclude, current legislative frameworks still require some development to fully fortify jurisdictions against the risks of cryptocurrencies. A global legal framework will allow this to be done in a more expedient manner, concomitantly preventing developing countries from being exploited due to their weaker legislative frameworks.