Master's Thesis

European Master in Law and Economics (EMLE)

University of Hamburg

Examining the Effectiveness of Cryptocurrency Regulation: Using Terrorist Attacks as a Probe

JEL-codes: K20, K29

Keywords: Cryptocurrency Regulation, Terrorism Financing

14 August 2024

Xiaoqing Huang

EMLE ID:

xiaoqing.haung@emle.eu

AUTHORSHIP DECLARATION

I hereby declare and confirm that this thesis is entirely the result of my own work except where otherwise indicated. I acknowledge the supervision and guidance I have received from Prof. Roee Sarel. This thesis is not used as part of any other examination and has not yet been published.

Xiaoqing Huang

14.08.2024 – Xiaoqing Huang

ABSTRACT

This study aims to examine the effectiveness of cryptocurrency regulations, specifically those targeting at terrorism financing and money laundering, in disrupting terrorism financing and thereby reducing the frequency and brutality of terrorist attacks. Utilizing a country-month panel dataset from 19 countries spanning August 2015 to June 2021, and considering that cryptocurrency regulations have worldwide spillover effects, this research employs a DID model with cryptocurrency adoption levels in different countries as a continuous treatment. The findings reveal that: (1) the studied regulations have not significantly reduced the overall frequency of terrorist attacks, including capital-intensive attacks; (2) however, a globally intensive regulatory period between December 2017 and June 2018 was associated with a decrease in the brutality of the attacks; and (3) in contrast, other isolated AML regulations launched by a single country had no effect on the brutality of attacks. The results provide empirical evidence for the importance of global cooperation in regulating cryptocurrency markets, particularly when countries are under-incentivized to launch non-excludable regulation under prisoners' dilemma.

CONTENTS

1. Introduction

Terrorist groups publicly shew their interest in cryptocurrency to raise fund at the earliest in 2013, where a Deep Web page entitled “Fund the Islamic Struggle without Leaving a Trace” invited donation by Bitcoin (Weimann, 2016). Reports indicate that cryptocurrency has been used to transfer funds to armed groups, finance terrorist activities and serve as the payment method for fraud and ransom (Brown, 2016; Hampton & Baig, 2015; Hasbi & Mahzam, 2018). Recently, Israeli authorities seized $1.7 Million to disrupt Hezbollah and Iran Quds Force’s financing by cryptocurrency exchanges in 2023 (Chainalysis, 2023), further highlighting the tangible and pressing nature of this concern.

It appears that cryptocurrency offers new opportunities for terrorist groups, prompting governments to impose general anti-money laundering (AML) regulations[1] on cryptocurrency to prevent its misuse. The ultimate goal of these regulations is, as always, to prevent terrorist attacks. Assuming that cryptocurrency is involved in terrorism financing, and if the regulations are effective, it is possible to expect some variation in the frequency or severity of terrorist attacks following the implementation of these regulations. Therefore, this research aims to empirically test the effectiveness of relevant cryptocurrency regulations by examining their impact on terrorist attacks.

The causal link between regulation and terrorist attacks is complex. However, the spillover effect of cryptocurrency regulations, particularly those targeting AML issues, allows us to observe the impact at a global level, especially when multiple countries implement regulations simultaneously. In such cases, the global influence of regulation and its varying effects on countries with different levels of cryptocurrency adoption create an a quasi-natural

[1] Although AML and counter-terrorist financing (CTF) are distinct activities, they share similar tactics and characteristics, and their strategies can often be applied interchangeably. This research also use the AML and CTF concepts interchangeably.

experiment. This research employs a Difference-in-Differences (DID) method to analyze the effectiveness of these regulations in reducing terrorist activities.

The research is structured as follows. Section 2 provides a literature review, examining current empirical studies on the relationship between terrorism financing and cryptocurrency, as well as the impact of cryptocurrency regulation. The review reveals that no existing studies directly addressing the intersection of these two fields. Section 3 constructs the theoretical framework to illustrate the link between terrorist financing and cryptocurrency regulation. It addresses three key questions: how terrorist groups fund their attacks; how and to what extent cryptocurrency is involved in terrorism financing; and how AML regulations function to disrupt these financing mechanisms with the spillover effect. Section 4 outlines the research design. This study employs a DID with a continuous treatment variable. Given the spillover effects of regulation, the research uses the extent to which each country is affected by the regulation as the treatment variable. Section 5 details the selection of measurements for different variables and describes the data collection process. Section 6 presents the empirical results, including findings from simple regressions as exploratory analyses, the parallel trend hypothesis test for the subsequent DID model, and the DID model itself. Section 7 discusses potential reasons for the insignificant results in models using the number of attacks as dependent variables. It further advocates for globalized regulation based on the comparison of effectiveness between isolated regulation and intensive regulation at a global level. Section 8 concludes the study.

2. Literature Review

2.1 Terrorism Financing in the Age of Cryptocurrency

Abundant empirical researches have explored the impact of terrorist attacks on the cryptocurrency market, focusing either on the overall market return or specifically on the price and trading volume of Bitcoin. However, fewer empirical researches examine how changes in cryptocurrency market contribute to terrorist attacks, particularly whether and to what extent cryptocurrency is utilized by terrorist groups. Most researches remain theoretical and is based on anecdotal evidence.

Amiram et al. (2022) observed a sharp rise in cumulative abnormal trading volumes of Bitcoin in the period before notable attacks, while such trend is insignificant in the vicinity of small attacks. In addition, they found that the abnormal volumes are concentrated in exchange and mixer accounts, indicating that terrorists mainly focus on converting cryptocurrency into fiat currency and laundering money.

Similarly, Sezgin & Özdurak (2023) identified that major attacks causing more than 100 deaths generate positive abnormal returns in the Bitcoin market 30 days prior to the attack, while a negative abnormal return is observed 10 days after the attack. Compared to Bitcoin, NFTs are more effected by attacks. They contend that changes in return are due to funding through the purchase of Bitcoin and NFTs to prepare for the attacks. When the funding stops, the negative abnormal return occurs in post-attack period.

In line with the previous researches, Akcinaroglu & Shi (2023) demonstrated that in every country, cryptocurrency popularity (measured by Google Trends score) is positively correlated to the number of terrorist attacks, while the volatility of price negatively related to the number of terrorist attacks.

In contrast, Song et al. (2023) found that Bitcoin price has almost no impact on the occurrence or brutality of terrorist incidents. They conclude that Bitcoin is not an effective means for terrorism financing. Plausible explanation includes the difficulty of converting Bitcoin to fiat currency, its pseudo-anonymity and volatility.

Lee & Choi (2021) found that although cryptocurrency prices do not influence terrorist attacks in short -term, a long-time effect can be identified from 2010-2017. Similarly, Majumder et al. (2019) shew that despite a long-run association between terrorist attacks and Bitcoin trading volumes in a 12-country panel from 2010-2016, there is no causality on either sides.

In general, empirical studies on terrorism financing and cryptocurrency are rather inadequate due to the scarcity of data. For this reason, most existing empirical evidence merely highlights correlations between terrorist attacks and cryptocurrency prices or trading volumes, often lacking thorough and convincing explanation. Moreover, the results on this topic are mixing. While the majority of studies confirm a potential interaction between the cryptocurrency market and terrorist attacks, contrary findings largely stem from differences in measurement and research methods.

2.2 The Impact of Cryptocurrency Regulation

A substantial body of theoretical research has been published discussing cryptocurrency regulation. At the broadest level, the debate can be divided into two main categories: “mainstream risk-averse regulation bulls” and “crypto-anarchist regulation bears” (Shanaev et al., 2020). More specifically, researchers have discussed the appropriate forms of regulation, exploring issues such as direct versus indirect regulation. Direct regulation focuses on targets the industry itself or the activities performed by entities within that industry, while indirect regulation focuses on the creditors and counterparties of entities in the regulated industry (Nabilou, 2019). Additionally, the debate extends to local versus global regulation. Local regulation is claimed to be sensitive to specific local needs, less influenced by geopolitical tension, involves lower switching cost and increases diversity within financial system. Regulation at global level leads to lower transaction cost between trade relationships, reduce local regulators' deficits and promote network effects by creating synergies (Sarel et al., 2023).

Some empirical studies examined the impact of regulatory announcements and enforcement on cryptocurrency trading prices and volumes. Fry & Cheah (2016) assessed the impact of several significant events up until 2014 on Bitcoin prices, finding mixed results across different events. For example, the prohibition of Chinese financial institutions from using Bitcoin and the closure of the Silk Road website[2] had significant shocks on the Bitcoin market.

Auer & Claessens (2018) compiled a database of 151 regulatory announcements from 2015 to 2018. They found that favorable regulatory announcements increased abnormal market returns, while unfavorable announcements decreased abnormal market prices.

Borri & Shakhnov (2020) analyzed the effects of China's 2017 ban on cryptocurrency on Bitcoin trading volumes. Their findings revealed that the Chinese regulation not only dramatically affected the domestic coin market but also had spill-over effects globally, leading to increased trading volumes in Korean won, Japanese yen, and U.S. dollars. Notably, most decreases in trading volumes occurred several months before the official announcement, suggesting that traders responded proactively to regulatory trends.

Shanaev et al. (2020) employed a more detailed categorization, identifying regulations from 2017 to 2019 as AML, exchange regulation, issuance regulation, risk concerns, and state-backed issuance of cryptocurrencies. They found that AML regulatory announcements and coin issuance regulations impacted market prices, while other types of regulations did not.

[2] A black market website which utilizes cryptocurrency as payment method.

Feinstein & Werbach (2021) explored the impact of a broader array of regulations worldwide, including bespoke regulatory developments, the official acknowledgment of cryptocurrency's status as either securities or currencies, AML and anti-fraud regulations and enforcement, and usage restrictions. When considerting country-level trading volume, they found no systematic movement of trading volume from one jurisdiction to another for Bitcoin and Ethereum following regulatory announcements. A weak impact of AML regulation on Ethereum trading movement was detected at the $p = 0.10$ level. When considering global trading volumes, no significant change was observed for Bitcoin, while Ethereum's global trading volume showed a statistically significant increase.

Among these studies, only two considered the impact of cryptocurrency regulation on terrorism financing. Amiram et al. (2022) found illicit funds are more likely to flow through unregulated exchanges rather than regulated ones. Akcinaroglu & Shi (2023), using Propensity Score Matching, found that countries with regulations designed to hinder terrorism financing experience fewer attacks than those without such regulations.

In sum, existing researches regarding the impact of crypto regulation primarily focuses on market return, price and trading volume. The findings can be summarized as follows: First, hard bans in regions with high trading volumes lead to significant decrease in both price and trading volume, as evidenced by China's ban on ICOs and the closure of exchanges. Second, different types of regulation should be examined separately. Not all regulation provoke reactions from cryptocurrency traders, but AML regulations appear to have a more significant impact than other forms of regulation.

2.3 Research Contribution and Novelty

One of the primary goals of cryptocurrency regulation is to curb money laundering activities within the market, particularly those conducted by terrorist groups. However, no research to date has directly linked the outcomes of terrorism financing—namely, terrorist attacks—to cryptocurrency regulation. This research bypasses the regulation's impact on the cryptocurrency market itself, instead focusing directly on its impact on terrorist attacks. By doing so, it offers a new perspective for evaluating the effectiveness of these regulations and provides a potential method for investigating the extent of terrorism financing through cryptocurrency.

3. Theoretical Mechanism

This research seeks to answer a critical question: Are cryptocurrency regulations effective in reducing terrorism attacks on a global scale? The causal link between cryptocurrency regulation and terrorism financing is complex and unfolds in three stages. First, it examines how terrorism funds contribute to attacks. Second, it explores the extent to which cryptocurrency is involved in terrorism financing. Finally, it assesses whether cryptocurrency regulation is effective in curbing terrorism financing.

This section of the essay explores the theoretical mechanism underlying terrorism financing, cryptocurrency, and its regulation. It begins by presenting the basic structure of terrorism financing. Next, it analyzes how and to what extent terrorist groups leverage cryptocurrency to their advantage. Finally, it delves into the features of AML regulation, offering a law and economics analysis of AML regulation in the context of cryptocurrency.

3.1 Terrorism Financing Flow

To understand how cryptocurrency can be involved in terrorist attacks, it is essential to first comprehend the funding mechanisms of terrorist groups. The financial flow within these groups typically consists of three stages: receipt, management/transfer, and spending (Dion-Schwarz et al., 2019). Initially, terrorist organizations raise funds from various sources, including charities, state sponsors, personal donations, and illicit activities (Biersteker et al., 2008).

Then, the movement of money is a crucial intermediate step, as a portion of the funds originates from locations different from the groups' bases and the sites of planned attacks. Traditionally, there are six widely accepted methods for transferring terrorism funds: cash couriers, informal transfer systems (e.g., hawala), money service businesses, formal banking, false trade invoicing, and high-value commodities (Freeman & Ruehsen, 2013). Groups that raise funds through illicit activities, such as drug trafficking, have an especially pressing need to circulate their illicit funds.

These funds are then allocated either to internal management—including recruitment, training, and services—or to executing attacks. Direct costs include expenditures directly associated with carrying out attacks, such as purchasing weapons used in the operations. Indirect costs involve maintaining the function of terrorist groups, including salaries, communication, training, travel and logistics, and advertising and recruitment. While direct costs are obviously linked to attacks, they are surprisingly much lower than indirect costs. For instance, the 9/11 attacks are the only significant attack with costs in the six-digit range, estimated between $300,000 and $500,000 (Kiser, 2005). Other attacks, such as the 2004 Madrid Railway bombings, cost approximately $10,000, and the 2005 London subway bombings cost only £8,000. Meanwhile, Al-Qaeda is estimated to have an annual financial flow of $20-50 million (Schneider, 2010). Indirect costs, therefore, are more critical to the survival of terrorist groups (Haigner et al., 2012).

Some may question whether terrorism financing truly impacts the frequency of attacks, given that such attacks can often be carried out at a low cost. However, empirical evidence suggests otherwise. Limodio (2022) found that funding significantly influences the frequency of attacks; when funding is adequate, the number of attacks tends to increase within a given time and location. Disrupting terrorism financing not only reduces the ability to spend illicit funds directly on attacks but also hampers the daily operations of terrorist groups. If a group experiences a financial shortfall, it may impair their overall functionality, ultimately hindering their capacity to carry out attacks.

3.2 How Cryptocurrency engages in Terrorism Financing

Current news and media reports suggest that cryptocurrency facilitates the operations of terrorist groups and is utilized at every stage of their funding processes. First, terrorist groups raise funds by soliciting donations in cryptocurrency, leveraging its security and anonymity. For instance, the U.S. Department of Justice (DOJ) recently disrupted a funding campaign involving the al-Qassam Brigades (Hamas's military wing), al-Qaeda, and the Islamic State of Iraq and the Levant (ISIS), seizing millions of dollars and over 300 cryptocurrency accounts (United States Department of Justice, 2020b). Several other cases have also demonstrated that individuals use cryptocurrency accounts to donate to terrorist groups (United States Department of Justice, 2020a). Additionally, in response to the impact of COVID-19 and fluctuating oil prices, terrorist groups have recognized the importance of diversifying their investment portfolios and developing their own means of funding (Bauer & Levitt, 2020). Cryptocurrency investment and mining have emerged as ideal methods to mitigate the risks associated with fiat currency and to generate revenue (Whyte, 2023).

Second, cryptocurrency provides a secure and efficient method for transferring money across borders. As the formal banking system has become increasingly regulated, with a heightened focus on anti-money laundering enforcement since 9/11, cryptocurrency has emerged as an excellent substitute. By design, cryptocurrency offers a secure method of transferring wealth, with anonymity that allows terrorist groups to obscure their funding sources. New generation of coins like Zcash and Ethereum provide more secured technology (Wood, 2014; Zhong, 2002).Transactions are irrevocable and require a private key, adding an additional layer of security. Moreover, the transfer costs for cryptocurrency are minimal, often close to zero. Cryptocurrency can be stored in online exchanges and wallets, or offline in flash drives. For online transfers, traders in different jurisdictions can move coins from one exchange to another without the capital control restrictions and scrutiny typically associated with fiat currency.

Third, terrorist groups use cryptocurrency to fund attacks. For example, it is used to purchase weapons on dark markets such as Silk Road (Weimann, 2016).

However, researchers have long questioned the actual extent to which cryptocurrency funding is feasible and decisive for terrorist groups (Dion-Schwarz et al., 2019; Goldman et al., 2017). Concerns exist at all three stages of the funding process. In terms of sources, individual Bitcoin donations are believed to constitute only a small portion of terrorism funding, especially when compared to state sponsorship, taxation, and profits generated from national resources in controlled territories.

Cryptocurrency is not flawless for money transfers either. Anonymity is not a feature of every type of coin. Bitcoin, for example, is only pseudonymous, as the addresses of senders are recorded and can potentially be traced back to their true identities (Goldman et al., 2017). Although the owner's identity is masked by a key, if the owner publishes the key for others to send them money, their identity can still be verified. Additionally, security is not guaranteed due to the decentralized nature of the cryptocurrency system. Unlike traditional banking systems, cryptocurrency wallets are individually controlled, making them vulnerable to cyber attacks (Covert, 2011). Moreover, technological methods to enhance security are not accessible to everyone.

Finally, the role of cryptocurrency in spending is less significant than commonly assumed. Most terrorist groups operate in regions with poor infrastructure and telecommunications, which limits the usability of cryptocurrency. They cannot easily use cryptocurrency for payments or convert it into local currency (Dion-Schwarz et al., 2019). Therefore, it is unlikely that cryptocurrency is used as a payment method for the daily maintenance of the group, as indirect costs.

Overall, the understanding of cryptocurrency's role in terrorism financing is largely shaped by published news and fundraising websites, which brings availability bias. While Bitcoin fundraising campaigns are easily observed on social media, the proportion of funding received from Bitcoin compared to other sources is less visible. As a result, Bitcoin may be perceived as a major source of terrorism financing. Although evidence indicates that terrorist groups are using cryptocurrency for financing, the extent of its involvement remains unclear. It is possible that the role of cryptocurrency in terrorism financing is overstated and stigmatized, leading to heightened public concern driven by media exposure.

3.3 AML Regulation for Cryptocurrency

3.3.1 Economics Rationale Behind Regulation

Ogus (2004) defined regulation as measures taken "to correct perceived deficiencies in the market system in meeting collective or public interest goals." Under the public interest theory of regulation, regulators aim to address collective goals when faced with market failures. Market failures include, but are not limited to, the under-provision of public goods, monopolies, externalities, and information deficits. Cryptocurrency presents several such market failures, necessitating regulations designed to address these issues.

First, the connection between fraud and cryptocurrency is rooted in information asymmetry and adverse selection. The anonymity and online nature of cryptocurrency transactions make it difficult to signal the credibility of trading parties. Information asymmetry exists between traders with illegal intentions and those with legitimate purposes. When honest traders repeatedly fall victim to fraud or when potential new entrants are deterred by negative news about cryptocurrency, they may exit the market, leaving a higher proportion of illicit traders. Regulation is needed to provide safeguards for participants in the cryptocurrency market and to signal credibility to legitimate traders. Moreover, the facilitation of terrorism financing is an unintended consequence of cryptocurrency, representing a negative externality. The cryptocurrency market generates profits for terrorist groups, enabling them to launch costly attacks that cause casualties and damage. Similarly, concerns such as financial stability

(Committee on Payments and Market Infrastructures, 2015), consumer protection (He & Habermeier, 2016) and taxation problems are other externalities associated with cryptocurrency. These challenges arise when the virtual world intersects with reality.

3.3.2 The Framework of AML Regulation in Cryptocurrency World

As discussed in Section 3.1, the primary function of cryptocurrency for terrorist groups is to facilitate the transfer of funds while evading detection. This section provides a detailed explanation of how cryptocurrency is utilized by money launderers and offers an overview of the current regulatory landscape.

Money laundering is the act of disguising the illegal origins of assets and income by creating seemingly legitimate processes and paper trails that make these funds appear lawful (Taylor et al., 2018). The process consists of three stages: placement, layering, and integration. Placement involves introducing illegal assets into the formal financial system. Layering is the process of obscuring the funding source and concealing the identity of the transferor. Integration is the final stage, where illegal funds are spent on legitimate assets and properties, effectively re-entering the legal financial system (H.-M. Wang & Hsieh, 2024).

In the context of cryptocurrency, there are two primary ways in which tokens are linked to illicit funds. First, funds that need to be laundered are generated from outside the cryptocurrency system. Criminals then integrate these illicit funds into the cryptocurrency network, exploiting its favorable features to obscure the sources. Second, illegal activities can directly generate tokens. For example, scams and fraud schemes often use cryptocurrency as a payment method.

Cryptocurrency operates as an informal payment system. Traders can either conduct transactions solely within this system, creating a closed-loop, or engage with the formal financial system outside the cryptocurrency network, forming an open-loop. In a fully closed-loop system, it is difficult for countries to exert effective control. However, due to the limited global acceptance of cryptocurrency across various sectors, there is often a need to exchange crypto for fiat currency. Once the internal loop of cryptocurrency interacts with the external formal financial system, opportunities arise to impose AML regulations (Dostov & Shust, 2014).

Some plausible AML regulations in the cryptocurrency world include the following: (1) Targeting Users and Traders: This approach involves applying Know Your Customer (KYC) requirements to the cryptocurrency field. While this imposes due diligence obligations on cryptocurrency businesses, the inherently anonymous nature of cryptocurrency poses challenges for effective KYC investigations. (2) Regulating Blockchain Service Providers: Instead of focusing on identifying individual cryptocurrency transactions, regulators can target blockchain service providers. This approach is widely used and will be discussed in more detail below. (3) Developing a Blacklisting System: A blacklisting system draws attention to suspicious cryptocurrency addresses. By publishing lists of addresses associated with illegal activities, this approach helps to mitigate information asymmetry among cryptocurrency market participants and prevents illegal activities from entering the market (H.-M. Wang & Hsieh, 2024).

Most AML regulations aim to disrupt the process of money laundering by regulating intermediaries in the cryptocurrency market. Table 1 illustrates the main intermediaries in the cryptocurrency market and their respective functions (Haffke et al., 2020).

TABLE I CRYPTOCURRENCY INTERMEDIARIES AND FUNCTIONS

Intermediaries	Functions
Initiator/issuers	Set up blockchains and give away/sell new tokens.
Miners	Create new block on blockchain and get new tokens as reward.

Exchanges	Provide conversions between fiat-crypto, crypto-crypto and crypto-fiat.
Mixing service	Break transaction into several small amount sub-transactions.
Wallet providers	Store or provide means for users to store their private key.
Tumbler services	Help users to disguise the origin of tokens.

Most current regulations target cryptocurrency exchanges because they serve as the bridge between the internal cryptocurrency loop and the broader financial system. For terrorist groups, exchanges are crucial since they still require fiat currency in many contexts, particularly in countries with lower levels of cryptocurrency adoption. Additionally, when using exchanges for transactions, individuals must also engage with a publicly distributed ledger, which allows others to trace their activities, thereby increasing the risk of identity theft and other security issues (Seo et al., 2018). To address these concerns, a service known as “mixing” was developed (Liu et al., 2021). Mixing services break down a transaction into several smaller sub-transactions, increasing the security and making it more difficult to trace the funds back to the original sender. This process aligns closely with the layering stage of money laundering, where the aim is to obscure the origins of illicit funds (Liu et al., 2021). To further enhance anonymity and complicate traceability, senders can use mixing services multiple times, creating multi-level layering.

However, regulation appears to be inherently incompatible with the fundamental features of cryptocurrency. Regulation is a form of control imposed by a governing authority to address market failures, relying on the state’s power to sanction or reward those who do or do not comply. In essence, regulation is inherently centralized, whereas the decentralized nature of cryptocurrency presents a significant challenge to regulatory efforts (Nabilou, 2019). For example, Know-Your-Customer (KYC) procedures require the disclosure of the identities of coin owners, which undermines the anonymity that is a core characteristic of cryptocurrency.

This tension between regulation and the decentralized nature of cryptocurrency complicates the effectiveness of regulatory measures. Moreover, rapid innovation in technology poses challenges to regulation. An international AML regulatory hierarchy strike a balance between finance innovation and market integrity (Roide, 2022).

3.3.3 Spillover Effect, But Limited

Controlling terrorism financing through cryptocurrency is a field where regulatory actions by one country create externalities for other countries. It combines the nature of cryptocurrency regulation with global counter-terrorism financing (CTF) efforts. Even when a country imposes regulations confined to its own jurisdiction, the effects can extend globally. However, the spillover effect is limited if only one country takes action. Below, I will provide the theoretical basis to argue that while a spillover effect does exist, it remains limited when regulatory efforts are fragmented. To maximize effectiveness, a global synergetic effort is essential.

First, cryptocurrency regulations are deemed to have spillover effect. A public blockchain is considered a non-excludable good, meaning that players—including exchanges and mixing services that are the most relevant for money laundering—from any country can participate in this market. Although laws and regulations imposed by one country may only directly apply to players within its jurisdiction, they also indirectly affect other traders utilizing the same blockchain in different countries (Sarel et al., 2023). National regulations on cryptocurrency trading, therefore, have global spillover effects at global level (Feinstein & Werbach, 2021). For instance, traders in Country A may choose to buy crypto assets on exchanges based in Country B, as they can access any exchange online. Consequently, regulations imposed on exchanges in Country B will directly impact traders in Country A.

The threat of money laundering and terrorism financing is global in nature, too. If one country effectively enforces strict AML regulations, the positive impact extends to the rest of the world (Colella et al., 2024). For example, if a country that was previously a safe haven for illicit funds suddenly imposes the strictest AML regulations—requiring the identification of customers behind transactions and blocking all suspicious deals—many criminal organizations operating globally would experience a significant disruption in their financing.

Terrorism financing through cryptocurrency combines the international characteristics of both the cryptocurrency market and money laundering networks. The spillover effects make relevant regulations a non-excludable good. Regulators cannot confine the effects of such regulations within a specific jurisdiction. For example, a terrorist group based in Country A might convert illegal cryptocurrency income into legal fiat currency through an exchange based in Country B, where regulatory requirements are less stringent. The converted fiat currency is then used either for the group's daily operations or directly to fund attacks. These attacks do not necessarily have to occur in Country B, as the legitimate funds can be transferred to Country C. If Country B imposes strict regulations on exchanges, the impact of these regulations could affect terrorist attacks in Country C and disrupt the operations of the terrorist group in Country A.

However, it is unrealistic to expect that regulatory actions in a single country, implemented in isolation, will be sufficient to influence terrorist attacks on a global scale. If only one regulation is enacted during a certain period, it is unlikely to have a significant impact on the outcome variable. Since the benefits of regulation are shared by all countries, the problem of terrorist financing is a collective action issue (Clunan, 2006). A fragmented regulatory system often fails due to the lack of universal standards and regimes, non-enforcement in certain countries, and indifference by national financial regulators (Verdugo-Yepes, 2008). Additionally, when only one jurisdiction is making an effort, criminals can engage in regulatory arbitrage, particularly in the context of cryptocurrency.

In contrast, when several major countries in the cryptocurrency market implement a series of regulations intensively within a relatively short time frame, this coordinated effort can have a more noticeable impact on the outcome. Intensive national-level regulations from multiple key players are more likely to create global synergetic effects, significantly influencing the frequency of terrorist attacks.

4. Research Design

First, this essay employs a simple linear regression analysis as an exploratory step to investigate the relationship between the dependent variable—the frequency of terrorist attacks—and the explanatory variable—the adoption of cryptocurrency.

More importantly, this essay employs a differences-in-differences (DID) strategy with a continuous treatment variable. Traditionally, a standard DID strategy assumes that the treatment group is influenced by an intervention (e.g., regulation) while the control group remains unaffected, making the treatment a binary variable. However, in this research, clearly distinguishing between treated and untreated groups is challenging due to the spill-over effects of regulations imposed by one country on others (as explained in Section 3). The effects of regulations in one country cannot be confined solely to that country. Despite this, it is still possible to leverage the fact that countries are influenced to varying extents based on their level of cryptocurrency adoption. The extent to which a country is influenced by cryptocurrency regulation serves as the treatment variable.

A continuous treatment is superior to a binary treatment because it captures more variation (Callaway et al., 2024). This approach is widely accepted in many prestigious studies. For example, Nunn & Qian (2011) estimated how the introduction of potatoes increased population and urbanization by exploiting regional variation in the suitability for cultivating potatoes to complete a DID design. Regions more suitable for potato cultivation experienced greater population increases, with suitability serving as the intensity of treatment.

In this research, countries with higher cryptocurrency acceptance and usage are presumed to be more sensitive to regulatory constraints, thereby experiencing greater disruption in their cryptocurrency market and thus terrorism financing network. Terrorist groups are likely to generate more frequent and successful attacks when they have adequate funding (Acharya, 2009). In a given time and location, increased financing leads to higher probabilities, numbers, and casualties of terrorist attacks (Limodio, 2022). Cryptocurrency regulations, particularly AML/CTF regulations, are designed to block suspicious transactions, thereby reducing or at least slowing down the flow of funds for attacks. Assuming that terrorist attacks are significantly funded by cryptocurrency, the number of attacks should exhibit substantial changes in response to these regulations. Therefore, by comparing the frequency of terrorist attacks before and after the implementation of regulations in countries with varying levels of cryptocurrency usage, this research aims to evaluate the effectiveness of AML/CTF cryptocurrency regulations. The equation used in this analysis takes the following form:

(1)

$$Y_{it} = \alpha + \gamma Intensity_{it} + \delta Post_t \times Intensity_{it} + \theta_i + \lambda_t + X_{it} + \epsilon_{it}$$

where i indexes countries and t indexes for time period, each month from August 2015 to June 2021. Y_{it} represents the dependent variable, which aims to reflect the robustness of terrorism financing. In this research, it is proxied by the frequency and characteristics of terrorist attacks. The variable $Intensity_{it}$ is the continuous treatment, indicating the extent to which countries adopt cryptocurrency. $Post_t$ is a dummy variable that equals one for observations in the post-regulation period, and zero otherwise. $Post_t \times Intensity_{it}$ is the interaction term for DID design. $X_{it}$is control variable. This equation also includes and country fixed effect θ_i and time fixed effect λ_t.

The following section will discuss the appropriate measurements for the different variables included in the equation.

4.1 Dependent Variable

The dependent variable reflects the robustness of terrorism financing, which is proxied by the frequency of terrorist attacks. In addition to the total number of attacks, I propose three other more accurate measures for assessing terrorism financing, recognizing that not all attacks have the same dependency on cryptocurrency funding.

First, Limodio (2022) found that while funding influences the frequency of attacks, this effect is more pronounced in highly capital-intensive activities. Small-scale attacks, such as assassinations, do not rely heavily on abundant funding. Supporting this analysis, Amiram et al. (2022) observed that abnormal Bitcoin trading volume significantly increased before large-scale attacks, whereas this increase was less pronounced for smaller attacks. Their research provides solid evidence that terrorist groups are more reliant on cryptocurrency to facilitate major attacks rather than smaller, less costly ones. This is primarily because major attacks are more expensive, requiring greater expenditure on advanced facilities, perpetrator remuneration, and logistics. Consequently, when the flow of funds is disrupted by cryptocurrency regulations, major or capital-intensive attacks are expected to fluctuate more than smaller, less resource-dependent attacks.

Another important consideration is how to define capital-intensive or major attacks. The UN Security Council Committee identified attacks that employ vehicles, heavy arms, and explosives as capital-intensive, a definition utilized in Limodio's research (2022). On the other hand, Amiram et al. (2022) classified large-scale attacks based on media exposure, defining them as those with dedicated Wikipedia articles. This research adopts the first method, as it is more straightforward and rooted in the tangible costs associated with the type of weapons used, which provides a more accurate measure of capital intensity. Additionally, data on weapon types is more comprehensive and reliable for this analysis.

Second, since cryptocurrency offers an ideal means for transferring illicit funds across borders, attacks launched far from the home territory of terrorist groups are likely to rely more heavily on cryptocurrency financing. This assertion is supported by the findings of Amiram et al. (2022). Additionally, the low acceptability of cryptocurrency within the home territories of terrorist groups makes it less likely for them to use cryptocurrency for conducting local attacks. Therefore, attacks launched far from the home territory of terrorist groups (herein referred to as "foreign attacks") are expected to fluctuate more in response to cryptocurrency regulations than attacks occurring within the base regions of these groups.

Third, the brutality of attacks can serve as a proxy for the cost. When more advanced and large-scale weapons, such as bombs or biological weapons, are employed, these attacks tend to result in higher casualties. Therefore, it is reasonable to consider not only the frequency of attacks but also their outcomes, as the severity and impact of an attack can reflect its underlying financial investment.

4.2 Cryptocurrency Regulation

Not all forms of regulation are of interest in this study. Only those regulations aimed at addressing terrorism financing and those that create a worldwide effect, such that all countries can be considered as treated, are relevant.

The regulations of interest in this research are those targeting AML and complete bans on cryptocurrency. Cryptocurrency regulations address various market failures, with the most severe risk for terrorism financing being its suitability for transferring illicit funds, rather than for fund raising or spending. AML regulations directly address this market failure. A hard ban on cryptocurrency has the most significant impact because it completely shuts down the local market. For example, the closure of the Chinese crypto market had substantial effects on both the domestic market and international spillover effects, as found by Borri & Shakhnov (2020).

As discussed in Section 3.3.3, only a series of regulations intensively within a relatively short time frame To identify such a period of regulatory activity, it is necessary to consider all relevant regulations and their effective dates. This research utilizes a regulation dataset developed in a previous study, as will be explained in Chapter 5. Higher financing levels in a given time and location typically lead to more terrorist attacks. Therefore, since intensive global-level regulation hinders the financing process, I expect to observe a lower level of attacks following the implementation of such regulations. In contrast, single regulation imposed alone is not likely to create a detectable effect. The level of attacks should not change significantly when using the isolated regulation as cutoff period.

4.3 Continuous Treatment Variable

In a DID strategy with a continuous treatment, the treatment reflects the extent to which different units are influenced by the regulation. In our case, the treatment variable should capture how a country is affected by the regulation. A country with widespread cryptocurrency adoption is likely to be more sensitive to cryptocurrency regulations than a country with limited adoption. This variance creates the possibility of a quasi-natural experiment. Countries with higher cryptocurrency adoption are expected to experience more significant changes in the outcome variable during the post-regulation period. Therefore, the treatment variable must effectively reflect the popularity or usage of cryptocurrency within each country.

To sum up, based on the three dependent variables, the corresponding hypotheses are as follows:

H1: Countries with higher popularity of cryptocurrency experience more decrease in the frequency of total terrorist attacks after the implementation of cryptocurrency regulation.

H2: Countries with higher popularity of cryptocurrency experience more decrease in the frequency of capital intensive terrorist attacks after the implementation of cryptocurrency regulation.

H3: Countries with higher popularity of cryptocurrency experience more decrease in the brutality of attacks after the implementation of cryptocurrency regulation.

H4: The effect is significant only after the implementation of intensive, coordinated regulations by multiple countries, and not after isolated regulations enacted by a single country.

4.4 Parallel Trend Hypothesis

Traditional DID design requires the treatment group and control group have parallel trend in change of dependent variable before regulation. The parallel trend hypothesis test is more complicated in a DID with continuous treatment. Following the method developed by Nunn & Qian (2011), this research uses the following equation to test the relationship between explanatory vairable and outcome variable.

(2)

$$Y_{attack,it} = \alpha + \beta I_t \times Intensity_{it} + \theta_i + \lambda_t + X_{it} + \epsilon_{it}$$

The variables are the same. The only difference is the interaction term. In equation (1) I interact the treatment intensity variable with a post-regulation indicator variable. In equation (2) I interact the treatment intensity variable with each of the time dummy variable I_t (the same as time fixed effect variables). The coefficient of the interaction term represents the relationship between the treatment intensity and the dependent variable in each month.

5. Data

5.1 Terrorist Attacks

The data on terrorist attacks, serving as the dependent variable, is sourced from the Global Terrorism Database (GTD). The GTD is an open-source database developed by the University of Maryland, with its latest update in 2021. It is widely used and recognized in numerous academic studies, providing data on terrorism attacks up to June 2021. Given that the original database is at the event level, I have aggregated the data to the country-month level, where each observation represents the number of attacks in a single country within a month.

The GTD offers several variables that can be used as dependent variables in this analysis: (1) the number of attacks per month, (2) the number of capital-intensive attacks per month, (3) the number of foreign attacks per month, and (4) the number of casualties. However, due to a significant amount of missing data, the variable for foreign attacks was excluded from the analysis.

To identify capital-intensive attacks, I utilized the “attacktype” variable in the GTD. This variable categorizes attack methods, including assassination, hijacking, kidnapping, barricade incident, bombing/explosion, armed assault, unarmed assault, facility/infrastructure attack, and unknown. For the purposes of this study, bombing/explosion and armed assault attacks are classified as capital-intensive attacks.

For the number of casualties, I calculated the sum of the “nkill” variable, which records the number of confirmed fatalities for each incident, and the “nwound” variable, which captures the number of confirmed non-fatal injuries.

5.2 Cryptocurrency Regulation

Feinstein & Werbach (2021) compiled a comprehensive dataset of all regulatory events initiated by governments from 2010 to mid-2019. For the purposes of this research, only regulations from 2015 onward are considered relevant. Their dataset includes detailed information on announcements, enforcement actions, and the enactment of laws and regulations pertaining to cryptocurrency. These regulations were further categorized into seven categories: recognizing cryptocurrency as or as not securities, denying cryptocurrency as currency, AML enforcement, AML regulation, fraud enforcement, and bespoke licensing. However, not all of these categories are relevant to this research.

First, to align with the purpose of this research, only AML enforcement, AML regulation, and fraud enforcement regulations should be included. Although Feinstein & Werbach provided a comprehensive list of all regulations along with brief descriptions, they did not publish the details of how they categorized these regulations into the six parts. Therefore, I manually screened the AML-relevant regulations based on the descriptions provided in the original regulation table in Feinstein & Werbach's essay.

Second, to accurately estimate the reaction of cryptocurrency traders, Feinstein & Werbach included announcements of laws and regulations, even when such regulations had not yet been enacted. These announcements, however, cannot directly restrict terrorism financing flows. This research excludes all mere announcements and considers the actual enactment of regulations as the relevant event date. Announcements alone are too distant from the actual implementation of regulations, and terrorist groups are unlikely to adjust their existing financing methods in response to them, as they do not yet pose a concrete threat. I assume that once a regulation is published, it has an immediate effect. Although regulations are often not effective immediately after enactment—leaving a gap between the enactment and when they actually influence terrorist attack outcomes—the knowledge of impending regulations may prompt terrorist groups to take proactive measures. These groups may reorganize their financing networks to circumvent the regulations, such as by transferring funds through alternative methods (as discussed in Part 3, Theoretical Framework). While proactive conversion to traditional strategy is voluntary and not directly forced by AML regulations, it still disrupts the original money flow, thereby negatively impacting the frequency of attacks. Moreover, as previously explained in Chapter 4, the impact of regulation depends on the strength of the global synergetic effect. It is crucial to consider how many countries initiated regulatory activities within a similar timeframe, rather than simply counting the total number of regulations. The original data includes all regulations, even when they originate from the same country within the same month. It is a common occurrence, as countries often implement a series of actions toward cryptocurrency in a short period. In this research, such regulations from a single country within the same timeframe should not be counted as separate records. Therefore, I combined repeated records and only considered regulations initiated by different countries within the same period.

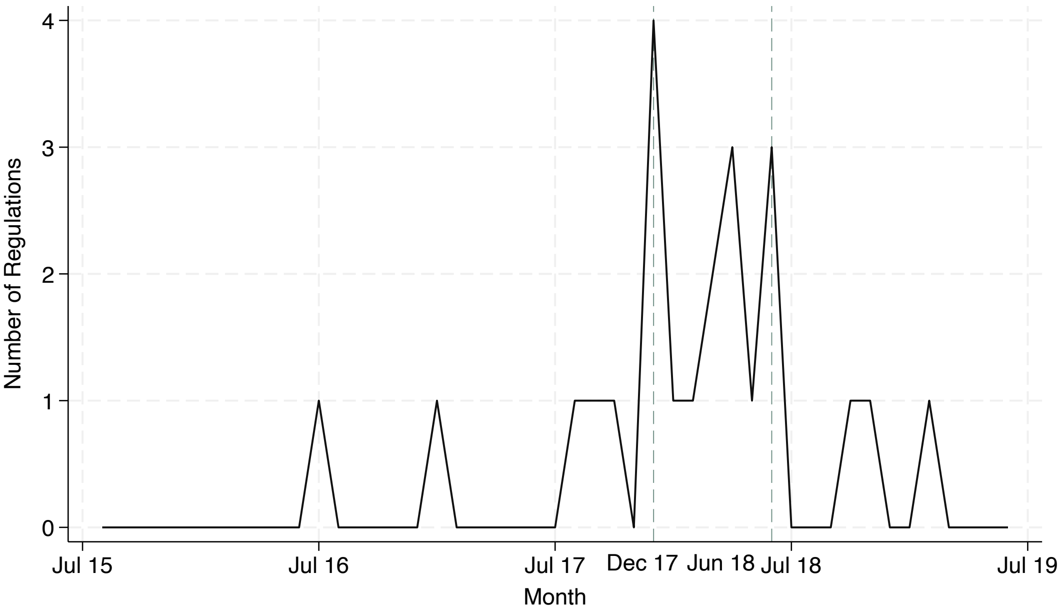
I manually screened these regulations. Table 2 contains all the cryptocurrency defined as relevant for terrorism financing.

TABLE II   RELEVANT AML REGULATIONS

Date	Country
2016/7/5	EU
2017/1/11	China
2017/8/16	Australia
2017/9/4	China
2017/10/10	Russia
2017/12/7	Indonesia
2017/12/14	Malaysia
2017/12/15	EU
2017/12/28	South Korea
2018/1/15	China
2018/2/12	Thailand
2018/3/7	Japan
2018/3/29	China
2018/4/6	India
2018/4/11	Australia
2018/4/22	Iran
2018/5/14	Zimbabwe
2018/6/12	South Korea
2018/6/12	Japan, UK, US
2018/6/22	Japan
2018/10/19	HK[晓清1]
2018/11/6	France
2019/2/25	Bahrain

Figure 2 displays the intensity of cryptocurrency regulation worldwide from July 2015 to June 2019. According to the graph, the period from December 2017 to June 2018 makes the time period when global regulatory activity concerning money laundering through cryptocurrency was particularly active. Prior to this, only individual countries enacted regulations sporadically in certain months. In December 2017, four countries implemented regulations in the same month, and this active regulatory trend continued until June 2018. If regulations are implemented by different country intensively in the same timeframe, their impact would be more pronounced and easier to capture.

FIGURE I GLOBAL CRYPTOCURRENCY REGULATION INTENSITY



Therefore, this research designates the period from December 2017 to June 2018 as the cutoff period for the DID analysis. Traditional DID designs typically use a single time point as the cutoff indicator. However, in this research, the effect of regulations extends over several months, making it challenging to select only one cutoff point. Consequently, this research will run the DID analysis based on all the time points within this 7-month period.

Additionally, other months where there was an isolated single regulation will be used as cutoff periods for comparison, allowing for an evaluation of the effects of intensive regulations versus isolated regulations. They are: July 2016 (EU), January 2017 (China), August 2017 (Australia), September 2017 (China), October 2017 (Russia), October 2018 (HK), November 2018 (France), February 2019 (Bahrain).

Another concern is the delay between the enactment of regulation and the subsequent effect on terrorist attacks. Amiram et al. (2022) observed significant increases in abnormal Bitcoin trading volume both 15 and 30 days before large-scale attacks. Similarly, Limodio (2022) noted an increase in attacks during the same month as an increase in financing, as well as in the subsequent month. However, since the cutoff point for this analysis spans several months rather than a single day or month, the use of seven DID models allows for a comprehensive examination of the effectiveness of regulations over the entire period. This approach accounts for the potential variability in timing between regulatory action and its impact on terrorism financing, making the exact timing less critical.

Finally, regulatory activities from mid-2019 to 2021 are not included due to time constraints, as there was not enough time to screen all relevant regulation news for this essay. This could be addressed in future research.

5.3 Intensity of Treatment

The intensity of treatment should reflect the extent to which a country is influenced by cryptocurrency regulation with a global effect. Ideal measures for this would be trading volume or adoption rate. Trading volume is directly related to the activity level of the cryptocurrency market in a country, and it may already include many small transactions used for money laundering. If cryptocurrency regulations are effective, countries with higher trading volumes are more likely to be significantly affected. However, due to data limitations, I was unable to obtain country-month-level trading volume data for cryptocurrency. The next best option is the adoption rate. Although some cryptocurrency analysis firms have published this data, it is only available at the annual level, which is incompatible with the country-month-level data used in this study.

Auer et al. (2022) published a database on the retail use of more than 200 crypto exchange apps at a monthly frequency between August 2015 and June 2022. Since the terrorism attack data is only available until June 2021, I utilized the data on app users from August 2015 to June 2021. While this measure is not perfect and less direct than trading volume or adoption rate, it still serves as a proxy for cryptocurrency popularity in a country. Smartphone applications are the most convenient way to engage in the cryptocurrency market, and the number of active users on these apps can reflect the level of participation in the cryptocurrency market to a certain extent. Moreover, exchanges are where cryptocurrency interacts with the broader financial system, and where money laundering activities often occur. Therefore, the number of active users on exchange apps can indicate a country's sensitivity to AML regulation.

Two important issues need further consideration. The first is heteroskedasticity, which refers to a systematic change in the spread of the residuals over time. I conducted the Breusch–Pagan/Cook–Weisberg test in Stata, and the results show a highly significant p-value, indicating a high level of heteroskedasticity. To address this, all subsequent regressions use clustered standard errors.

The second issue is potential endogeneity. Monthly active users of cryptocurrency exchange applications might be endogenous to terrorist attacks. Countries with more active users may be more technology-friendly and open to new changes, and this inclination toward novelty could potentially lead to increased vulnerability to terrorist attacks. To address the endogeneity problem, I identified two instrumental variables that are correlated with cryptocurrency adoption but not related to terrorist attacks, according to previous studies.

Given that the explanatory variable (monthly active users) is measured at the monthly level, at least one of the instrumental variables should also be at this level. This requirement makes the search for appropriate instrumental variables more challenging, as most available data is at the yearly level. Since these two instrumental variables are not perfectly randomly assigned, I use them as a robustness check rather than for the main analysis.

(1) Consumer Price Index (CPI): CPI is a common measure of inflation and has been shown to correlate with cryptocurrency usage (Auer et al., 2022). Some cryptocurrencies are viewed as a hedge against fiat currency, leading to increased investment during periods of higher expected inflation. However, the relationship between CPI and terrorist attacks is less

direct. Monthly CPI data was downloaded from the BIS Data Portal[3], though data for Turkey was missing. I supplemented this by obtaining the monthly CPI data for Turkey from the official website of the Turkish Statistical Institute.[4]

(2) Coal Consumption: Cryptocurrency mining is extremely energy-intensive, and electricity produced by coal is a key energy source. For example, Karmakar et al. (2021) note that Bitcoin mining now consumes around half as much electricity as the UK. In contrast, there is limited research on the relationship between coal consumption and terrorist attacks. The data on coal consumption is at the yearly level and was extracted from the website of the Energy Institute.[5]

5.4 Control Variables

Control variables account for other factors that affect the frequency of terrorist attacks across different countries over time. This research takes advantage of panel data by incorporating two-way fixed effects, which eliminate all time-invariant and unit-invariant effects. The use of fixed effects simplifies the selection of control variables. This research considers two variables that fluctuate over time and across countries: GDP and the unemployment rate. Both factors have been shown to correlate with the frequency of terrorist attacks in previous research (Korotayev et al., 2021).

GDP is a common indicator of a country's economic growth, and I applied a logarithmic transformation to reduce heteroskedasticity. The unemployment rate reflects the stability of society. While the mechanisms through which these two factors contribute to terrorism are complex, this research does not explore that question in detail. Both GDP and unemployment

[3] See https://data.bis.org/topics/CPI/data.
[4] See https://www.tuik.gov.tr/Home/Index.
[5] See https://www.energyinst.org/statistical-review/resources-and-data-downloads.

rate data are sourced from the World Bank Open Data.[6] Since month-level data is unavailable, both variables are measured at the yearly level.

The descriptive statistics summary is presented in Table III below.

TABLE III DESCRIPTIVE STATISTICS

VarName	Obs	Mean	SD	Max
Total attacks	1349	6.3988	16.3649	130.0000
Capital intensive attacks	1349	3.0956	9.3084	72.0000
Brutality	1349	13.5827	54.1000	932.0000
Monthly active users	1349	147.1624	316.0473	4511.9136
ln(GDP)	1349	28.2932	0.9780	30.7920
Unemployment rate	1349	7.4129	5.0104	28.7700

[6] See https://data.worldbank.org/.

6. Empirical results

6.1 Simple Regression

Table IV presents the results of simple regressions between the monthly active users of cryptocurrency exchange applications and the dependent variables depicting different aspects of terrorist attacks. However, the interpretation of these regressions is limited, as these models are merely exploratory. The relationship between cryptocurrency adoption and terrorist attacks is complex and influenced by many other confounding factors. Therefore, no firm conclusions can be drawn from these results alone.

For each dependent variable, I first estimated a model without control variables and then added all control variables in the second model. The constants in the models without control variables were significant but became insignificant after adding the control variables. This suggests that the control variables effectively addressed the omitted variable bias. Given that the data is panel data at the country-month level, two-way fixed effects were employed in all models. Country fixed effects (unit fixed effects) control for all time-invariant factors that differ between countries, while time fixed effects control for all country-invariant factors, including any events or trends that affected the severity of attacks across all countries. No observations were dropped in any of the models. However, if the coefficients are insignificant in the simple regressions, it is likely that the DID models will also yield insignificant results.

The coefficient for the explanatory variable—monthly active users—is not significantly related to either the total number of attacks or capital-intensive attacks. This insignificance is not surprising, as the mechanism for cryptocurrency-related terrorism financing is nuanced and subtle. It is unrealistic to expect a direct correlation between terrorism attacks and the monthly active users of cryptocurrency exchange applications. However, the results do not suggest that cryptocurrency has nothing to do with terrorism financing. Notably, monthly active users are significantly correlated with the brutality of attacks, at a significance level of $p<0.1$. The coefficient is -0.016, indicating that higher cryptocurrency adoption is associated with a decrease in the brutality (measured by the number of killed and wounded) of terrorist attacks.

TABLE IV
THE RELATIONSHIP BETWEEN CRYPTOCURRENCY APPLICATION MONTHLY ACTIVE USERS AND TERRORISM ATTACKS

	Dependent Variables					
	(1) total	(2) total	(3) capital intensive	(4) capital intensive	(5) brutality	(6) brutality
Monthly active users	-0.002	-0.001	-0.001	-0.001	-0.017*	-0.016*
	(-0.51)	(-0.48)	(-0.83)	(-0.87)	(-1.80)	(-1.96)
ln(GDP)		8.508		4.293		72.807
		(0.47)		(0.40)		(0.73)
Unemployment rate		0.008		-0.243		-3.044
		(0.01)		(-0.49)		(-0.82)
Constant	14.219**	-225.978	7.112**	-112.275	22.507*	-2,010.142
	(2.31)	(-0.45)	(2.33)	(-0.38)	(1.96)	(-0.72)
Observations	1,349	1,349	1,349	1,349	1,349	1,349
R-squared	0.092	0.097	0.096	0.103	0.073	0.090
Number of countries	19	19	19	19	19	19
Time FE	YES	YES	YES	YES	YES	YES
Unit FE	YES	YES	YES	YES	YES	YES
Instrument Variable	NO	NO	NO	NO	NO	NO
Standard Error	clustered	clustered	clustered	clustered	clustered	clustered

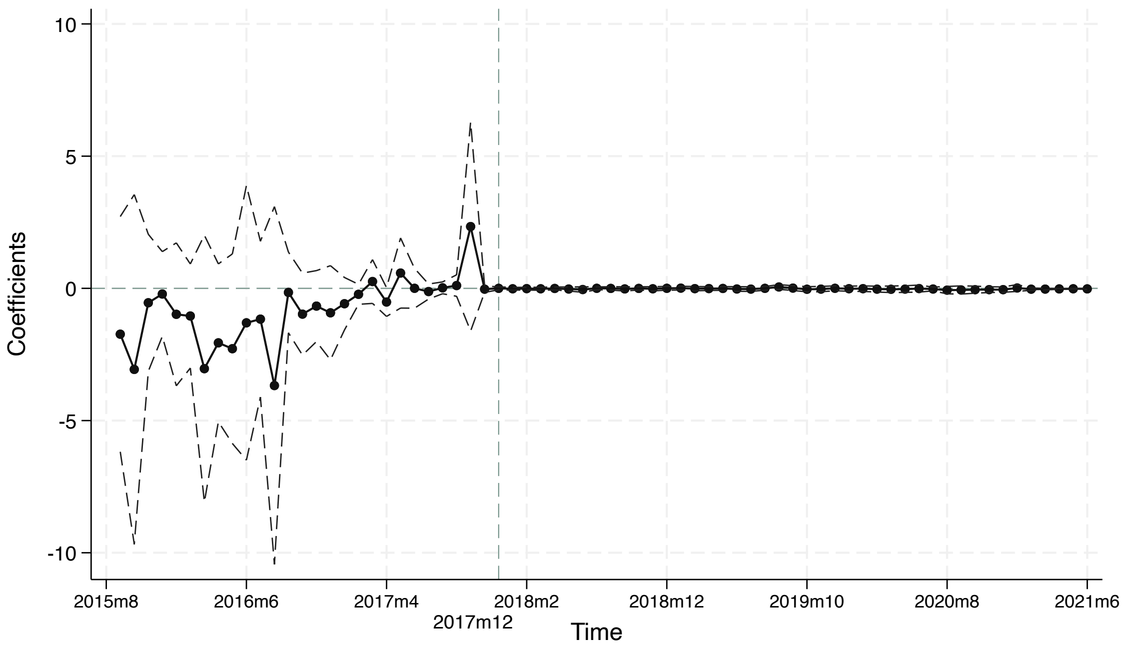
Robust t-statistics in parentheses *** p<0.01, ** p<0.05, * p<0.1

Notes: Observations are all country-month level. Time period is from Aug 2015 to June 2021. Nineteen countries are included. The dependent variable are total monthly attacks, capital intensive monthly attacks or brutality of attacks. Each of them has two models, one with control variable and one without control variables. All regressions include time and unit fixed effect. All regressions use clustered standard error.

6.2 Parallel Trend Hypothesis

The coefficient of the interaction term between the treatment intensity variable (monthly active users) and the time dummy variable represents the relationship between the dependent variable and treatment intensity for each month. Figure II illustrates the changes in this coefficient over the time span.[7] Although the coefficient is mostly insignificant across the months, there are still notable findings. Before December 2017, the coefficient was larger and experienced more fluctuations. After December 2017, the coefficient became much smaller, closer to zero, and remained constant at this level.

FIGURE II CHANGE OF ATTACK BRUTALITY WITH TREATMENT INTENSITY OVERTIME



The trend of the coefficient suggests that before December 2017, the impact of cryptocurrency adoption on the brutality of terrorist attacks was greater, though not significant, than it was afterward. The cutoff time closely aligns with the chosen cutoff period in this

[7] I did not examine the model when total attacks and capital-intensive attacks are dependent variable, since the coefficient is not significant in simple regression.

research. Therefore, it is reasonable to expect that the following DID model will detect significant changes before and after the period of active regulation.

6.3 DID With A Continuous Treatment

Tables V to VI present the results of the DID models, with brutality as the dependent variables. In Table V, the period from December 2017 to June 2018 was selected as the cutoff period because regulatory activities were most active during these seven months. Accordingly, I ran seven DID regressions, using each month within this period as a cutoff point. In Table VI, I choose the months when there is only isolated regulation by a single country, region or jurisdiction as cutoff period. Table VII to VIII present the results when the number of total attacks and capital-intensive attacks are dependent variables. All models include control variables, as well as unit (country) and time (month) fixed effects. The results are based on clustered standard errors.

As expected, the coefficient of the interaction term in the DID setting for both total monthly attacks and capital-intensive attacks is not significant.

However, when the outcome variable is brutality, the coefficient for the interaction term is significant in most cases. In column (1), with a cutoff time of December 2017, the interaction term coefficient is -0.158, significant at the $p<0.1$ level. In column (2), with a cutoff time of January 2018, the interaction term coefficient is -0.07, significant at the $p<0.05$ level. In columns (3) through (5), the interaction term coefficient decreases from -0.052 to -0.039, remaining significant at the $p<0.1$ level. However, in columns (6) and (7), where the cutoff time is June 2018, the interaction term coefficient is no longer significant.

Now turning to the coefficient of the monthly active users term, it is noteworthy that the positive coefficient is only significant at the $p<0.1$ level in columns (1) and (2).

For DID with a continuous treatment, the interpretation of the interaction term coefficient is not straightforward. The interaction term represents the relationship between cryptocurrency popularity (proxied by monthly active users) and the post-regulation indicator. The coefficient reveals the change in the outcome variables resulting from changes in cryptocurrency adoption after the active regulation period. Specifically, it measures the additional impact experienced by countries with higher adoption levels (compared to those with lower adoption levels) during the post-regulation period. A negative coefficient suggests that higher cryptocurrency adoption rates are associated with a larger decrease in brutality (measured by the number of killed and wounded in attacks) during the post-regulation period. The decreasing significance of the coefficient over time indicates that the effect of regulation is diminishing.

The interpretation of the coefficient for the active users term alone is also of particular interest for this research. This coefficient reflects the relationship between cryptocurrency adoption rates and terrorism in the pre-regulation period. It reveals the change in the outcome variables resulting from changes in cryptocurrency adoption before the active regulation period. A positive coefficient indicates that higher adoption rates are associated with a larger increase in brutality.

More importantly, both the interaction term coefficient and the coefficient for the active users term are insignificant when using single isolated regulation as cutoff period. This indicates that the effect of such isolated regulation is not significant.

To conclude, while the results do not support hypotheses H1 and H2, they do support H3 and H4. The regulations implemented between December 2017 and June 2018 have effectively impacted the outcomes of terrorist attacks by reducing the casualties caused by these attacks. In contrast, other isolated single regulations did not lead to such an effect.

TABLE V RELATIONSHIP BETWEEN CRYPTOCURRENCY APPLICATION MONTHLY ACTIVE USERS AND TERRORISM ATTACKS BRUTALITY AFTER *INTENSIVE REGULATION*

VARIABLES	(1) Dec 2017	(2) Jan 2018	(3) Feb 2018	(4) Mar 2018	(5) Apr 2018	(6) May 2018	(7) Jun 2018
ln(GDP)	79.486	76.052	75.414	75.067	74.955	74.715	74.399
	(0.79)	(0.76)	(0.75)	(0.75)	(0.75)	(0.74)	(0.74)
Unemployment rate	-2.855	-2.904	-2.907	-2.913	-2.910	-2.919	-2.936
	(-0.77)	(-0.79)	(-0.79)	(-0.79)	(-0.79)	(-0.80)	(-0.80)
ActiveUsers	0.143*	0.054*	0.036	0.026	0.023	0.017	0.011
	(1.86)	(1.81)	(1.42)	(1.28)	(1.25)	(0.92)	(0.60)
ActiveUsers$\times$ $Post_{Dec2017}$	-0.158*						
	(-2.01)						
ActiveUsers $\times$ $Post_{Jan2018}$		-0.070**					
		(-2.18)					
ActiveUsers$\times$ $Post_{Feb2018}$			-0.052*				
			(-1.86)				
ActiveUsers $\times$ $Post_{Mar2018}$				-0.043*			
				(-1.78)			
ActiveUsers $\times$ $Post_{Apr2018}$					-0.039*		
					(-1.79)		
ActiveUsers $\times$ $Post_{May2018}$						-0.033	
						(-1.49)	
ActiveUsers $\times$ $Post_{Jun2018}$							-0.027
							(-1.22)
Constant	-2,200.827	-2,103.097	-2,084.975	-2,075.090	-2,071.927	-2,065.067	-2,055.972
	(-0.78)	(-0.75)	(-0.75)	(-0.74)	(-0.74)	(-0.74)	(-0.73)
Observations	1,349	1,349	1,349	1,349	1,349	1,349	1,349
R-squared	0.094	0.092	0.091	0.091	0.091	0.091	0.090
Number of countries	19	19	19	19	19	19	19
Time FE	YES	YES	YES	YES	YES	YES	YES
Unit FE	YES	YES	YES	YES	YES	YES	YES
IV	NO	NO	NO	NO	NO	NO	NO
SE	clustered	clustered	clustered	clustered	clustered	clustered	clustered

Robust t-statistics in parentheses
*** p<0.01, ** p<0.05, * p<0.1

TABLE VI RELATIONSHIP BETWEEN CRYPTOCURRENCY APPLICATION MONTHLY ACTIVE USERS AND TERRORISM ATTACKS BRUTALITY AFTER *ISOLATED REGULATION*

VARIABLES	(1) Jul 2016	(2) Jan 2017	(3) Aug 2017	(4) Sep 2017	(5) Oct 2017	(6) Oct 2018	(7) Nov 2018	(8) Feb 2019
ln(GDP)	73.381	70.247	69.512	70.814	88.173	74.386	74.358	74.637
	(0.74)	(0.72)	(0.71)	(0.71)	(0.88)	(0.74)	(0.74)	(0.74)
Unemployment rate	-2.585	-2.632	-3.097	-3.083	-2.710	-2.927	-2.927	-2.900
	(-0.75)	(-0.76)	(-0.84)	(-0.83)	(-0.71)	(-0.80)	(-0.80)	(-0.80)
ActiveUsers	-1.563	-1.277	-0.208	-0.112	0.609	0.008	0.007	0.008
	(-1.31)	(-1.46)	(-0.95)	(-0.52)	(1.35)	(0.48)	(0.41)	(0.45)
ActiveUsers× $Post_{Jul2016}$	1.546							
	(1.30)							
ActiveUsers × $Post_{Jan2017}$		1.258						
		(1.45)						
ActiveUsers× $Post_{Aug2017}$			0.191					
			(0.88)					
ActiveUsers × $Post_{Sep2017}$				0.096				
				(0.45)				
ActiveUsers × $Post_{Oct2017}$					-0.620			
					(-1.39)			
ActiveUsers × $Post_{Oct2018}$						-0.025		
						(-1.11)		
ActiveUsers × $Post_{Nov2018}$							-0.024	
							(-1.03)	
ActiveUsers × $Post_{Feb2019}$								-0.025
								(-1.05)
Constant	-2,022.009	-1,934.614	-1,915.776	-1,953.110	-2,449.387	-2,055.664	-2,054.866	-2,062.950
	(-0.73)	(-0.71)	(-0.70)	(-0.71)	(-0.87)	(-0.73)	(-0.73)	(-0.73)
Observations	1,349	1,349	1,349	1,349	1,349	1,349	1,349	1,349
R-squared	0.096	0.101	0.090	0.090	0.105	0.090	0.090	0.091
Number of country_num	19	19	19	19	19	19	19	19
Time FE	YES	YES	YES	YES	YES	YES	YES	YES
Unit FE	YES	YES	YES	YES	YES	YES	YES	YES
IV	NO	NO	NO	NO	NO	NO	NO	NO
SE	clustered	clustered	clustered	clustered	clustered	clustered	clustered	clustered

TABLE VII RELATIONSHIP BETWEEN CRYPTOCURRENCY APPLICATION MONTHLY ACTIVE USERS AND TOTAL TERRORISM ATTACKS AFTER REGULATION

VARIABLES	(1) Dec 2017	(2) Jan 2018	(3) Feb 2018	(4) Mar 2018	(5) Apr 2018	(6) May 2018	(7) Jun 2018
ln(GDP)	8.107	8.223	8.326	8.354	8.359	8.266	8.213
	(0.44)	(0.45)	(0.46)	(0.46)	(0.46)	(0.45)	(0.45)
Unemployment rate	-0.003	-0.004	-0.001	-0.001	-0.001	-0.008	-0.012
	(-0.00)	(-0.00)	(-0.00)	(-0.00)	(-0.00)	(-0.01)	(-0.01)
ActiveUsers	-0.011	-0.008	-0.005	-0.004	-0.004	-0.006	-0.006
	(-0.87)	(-1.20)	(-1.17)	(-1.30)	(-1.39)	(-1.52)	(-1.49)
ActiveUsers× $Post_{Dec2017}$	0.009						
	(0.63)						
ActiveUsers × $Post_{Jan2018}$		0.006					
		(0.71)					
ActiveUsers× $Post_{Feb2018}$			0.004				
			(0.55)				
ActiveUsers × $Post_{Mar2018}$				0.003			
				(0.53)			
ActiveUsers × $Post_{Apr2018}$					0.003		
					(0.55)		
ActiveUsers × $Post_{May2018}$						0.004	
						(0.71)	
ActiveUsers × $Post_{Jun2018}$							0.005
							(0.76)
Constant	-214.526	-217.807	-220.739	-221.546	-221.676	-219.004	-217.474
	(-0.42)	(-0.43)	(-0.44)	(-0.44)	(-0.44)	(-0.43)	(-0.43)
Observations	1,349	1,349	1,349	1,349	1,349	1,349	1,349
R-squared	0.098	0.098	0.097	0.097	0.097	0.098	0.098
Number of countries	19	19	19	19	19	19	19
Time FE	YES	YES	YES	YES	YES	YES	YES
Unit FE	YES	YES	YES	YES	YES	YES	YES
IV	NO	NO	NO	NO	NO	NO	NO
SE	clustered	clustered	clustered	clustered	clustered	clustered	clustered

Robust t-statistics in parentheses
*** p<0.01, ** p<0.05, * p<0.1

TABLE VIII RELATIONSHIP BETWEEN CRYPTOCURRENCY APPLICATION MONTHLY ACTIVE USERS AND CAPITAL INTENSIVE ATTACKS AFTER REGULATION

VARIABLES	(1) Dec 2017	(2) Jan 2018	(3) Feb 2018	(4) Mar 2018	(5) Apr 2018	(6) May 2018	(7) Jun 2018
ln(GDP)	4.226	4.188	4.261	4.309	4.292	4.260	4.240
	(0.39)	(0.38)	(0.39)	(0.40)	(0.40)	(0.39)	(0.39)
Unemployment rate	-0.245	-0.248	-0.245	-0.242	-0.243	-0.246	-0.247
	(-0.50)	(-0.51)	(-0.50)	(-0.49)	(-0.50)	(-0.50)	(-0.51)
ActiveUsers	-0.003	-0.004	-0.002	-0.001	-0.001	-0.002	-0.002
	(-0.69)	(-1.16)	(-0.99)	(-0.82)	(-1.17)	(-1.48)	(-1.48)
ActiveUsers× $Post_{Dec2017}$	0.002						
	(0.30)						
ActiveUsers × $Post_{Jan2018}$		0.002					
		(0.55)					
ActiveUsers× $Post_{Feb2018}$			0.001				
			(0.22)				
ActiveUsers × $Post_{Mar2018}$				-0.000			
				(-0.15)			
ActiveUsers × $Post_{Apr2018}$					0.000		
					(0.01)		
ActiveUsers × $Post_{May2018}$						0.001	
						(0.26)	
ActiveUsers × $Post_{Jun2018}$							0.001
							(0.37)
Constant	-110.353	-109.278	-111.351	-112.743	-112.249	-111.319	-110.758
	(-0.36)	(-0.36)	(-0.37)	(-0.37)	(-0.37)	(-0.37)	(-0.37)
Observations	1,349	1,349	1,349	1,349	1,349	1,349	1,349
R-squared	0.103	0.103	0.103	0.103	0.103	0.103	0.103
Number of countries	19	19	19	19	19	19	19
Time FE	YES	YES	YES	YES	YES	YES	YES
Unit FE	YES	YES	YES	YES	YES	YES	YES
IV	NO	NO	NO	NO	NO	NO	NO
SE	clustered	clustered	clustered	clustered	clustered	clustered	clustered

Robust t-statistics in parentheses
*** p<0.01, ** p<0.05, * p<0.1

7. Discussion

Overall, the empirical results suggest three key conclusions: (1) cryptocurrency AML regulations do not influence the frequency of terrorist attacks; (2) however, the intensive AML regulatory activity between December 2017 and June 2018 significantly reduced the brutality of attacks; (3) in contrast, other isolated AML regulations have no effect on the brutality of attacks.

These findings yield two important lessons: first, cryptocurrency AML regulations do not impact the number of attacks; second, only regulations that are intensively implemented at a global level can make a meaningful difference. The following discussion will first explore the potential reasons for the insignificance of regulations concerning the frequency of attacks and then address the need for a globalized regulatory framework.

7.1 Challenges in Linking Cryptocurrency to Terrorism Financing

For cryptocurrency regulations to impact terrorist attacks, a long causal chain must be completed. If any stage in this chain is not fulfilled, it can result in an insignificant effect. Therefore, even if no effect is detected in this research, it does not negate the importance or potential impact of these regulations. At least three reasons can help explain the insignificant results.

First, one might question the actual extent of cryptocurrency's involvement in terrorism financing. Terrorist groups have increasingly diversified their funding sources and tools, with traditional financing methods (e.g., Hawala, physical transportation of currency) still playing a primary role in ensuring the smooth functioning of these groups (S. Wang & Zhu, 2021). Cryptocurrency may be over-stigmatized in the context of terrorism financing. However, this does not diminish the necessity of AML regulation in the cryptocurrency market. Beyond terrorist groups, international crime syndicates and even nations use cryptocurrency to launder money. In fact, terrorism financing accounts for only a small share of illicit transactions in the cryptocurrency ecosystem (Chainalysis, 2024).

Second, the effectiveness of regulations is often undermined by the problem of regulatory arbitrage. The globalized nature of the cryptocurrency market allows criminals to shift their activities to jurisdictions with lower compliance standards. Additionally, if cryptocurrency increasingly attracts regulatory attention, criminals can revert to traditional financing channels. These traditional methods are well-established, group members are more familiar with them, and the fixed costs associated with using them are lower.

Third, more radically, one might directly question the overall effectiveness of CTF measures. As detailed in Section 3.1, typical terrorist attacks are not expensive to carry out. Temporary disruptions caused by regulation may not immediately alter terrorist groups' decisions to launch attacks, as they have various methods to choose from. However, the most important role of CTF is to impede the financing flow of terrorist groups in the long term, which can gradually weaken their operational capabilities.

7.2 Challenges in Implementing Effective Crypto AML Regulation

While the empirical results suggest that a coordinated global regulatory framework may be the most effective solution, individual countries often lack sufficient incentives to act. In sum, the argument proceeds as follow: The non-excludable nature of cryptocurrency presents challenges in regulation, often resulting in either under-regulation or over-regulation. In the specific context of AML regulation for cryptocurrency, regulators face a prisoner's dilemma. Strict regulation can stifle innovation and increase compliance costs within their own jurisdictions, while the benefits of such regulation—such as reducing terrorism financing—are shared globally. The benefits of AML and CTF regulation represent a typical public good, leading to under-provision in the absence of effective global governance. The following sections will provide a detailed analysis of this argument.

7.2.1 DLT as Common Good

Distributed Ledger Technology (DLT) is the foundational technology that underpins cryptocurrency, with blockchain being the most common and widely used type of DLT supporting transactions in the cryptocurrency market. Blockchains can be either public, allowing anyone to join, or private, accessible only to authorized users (Miller et al., 2019). As explained by Sarel et al. (2023), when applying the taxonomy of goods[8] to blockchain, a public blockchain is non-excludable and seemingly rivalrous, classifying it as a common good. This means that one cannot prevent others from using the same blockchain, and each additional user can diminish the quality of the chain.

Different users from various jurisdictions converge on a single blockchain, forming a unified market. Regulations implemented by one jurisdiction may only directly affect the users within that jurisdiction, but since these users participate in the broader blockchain market, the regulations ultimately impact the market as a whole. Consequently, regulations imposed on public blockchains are also non-excludable. This non-excludable nature can lead to either over-regulation, resulting in high compliance costs, or under-regulation, leading to a free-rider problem, where jurisdictions wait for others to take action (Sarel et al., 2023).

The above analysis is based on the features of public blockchains. However, even beyond the context of public blockchains, the cryptocurrency market inherently operates on a global scale. In many other economic activities, trades are often constrained by geographical boundaries within specific jurisdictions. In contrast, the cryptocurrency market allows traders to access any exchange worldwide from their computers, with transactions not subject to

[8] Based on rivalry and excludability, economic goods consists of four categories, namely private goods, common goods, club goods and public goods.

traditional capital controls (Hougan et al., 2019). Compared to other economic activities, the cost of shifting cryptocurrency transactions to another jurisdiction is relatively low. This low transaction cost facilitates a global-level market for cryptocurrency, where trading activities across all jurisdictions are interconnected. Although transaction costs vary among different tokens (Sarel, 2021), these costs do not negate the global nature of cryptocurrency.

7.2.2 CTF as Public Good

In a highly decentralized global cryptocurrency market, regulations aimed at reducing terrorism attacks function as a public good. These regulations are non-excludable because no single country can prevent others from benefiting from the reduced flow of terrorism financing. They are also non-rival, as a decrease in the global frequency of terrorist attacks benefits all countries equally; the inclusion of additional countries in these efforts does not diminish the benefits for others.

Imposing strict AML rules is costly, not only in terms of enforcement but also because it increases transaction costs for businesses within a country. As a result, the country that imposes the regulation may suffer economic losses, while the benefits, such as reduced terrorism financing, might accrue to other countries.

In the context of AML regulation for cryptocurrency, countries face a prisoner's dilemma. Strict regulations may stifle innovation in emerging technologies, curb market activity, and increase transaction cost and compliance costs within their jurisdiction (Roide, 2022). Given the low cost for traders to switch jurisdictions, if one country imposes unfavorable regulations, cryptocurrency trading often shifts to another country. As cryptocurrency becomes a promising alternative to traditional currency, especially after COVID-19, countries are paying closer attention to its regulation. If one country opts for strict regulation while others do not, that country bears the costs alone, while the benefits—such as disrupting the financing flow of terrorist groups—are shared globally. For example, if Country A blocks suspicious transactions in its banks, the outcome could be that criminals in Country B experience a funding shortage. Meanwhile, it is Country A to bear the enforcement cost. Consequently, countries have low incentive to ensure strict enforcement AML within its own jurisdiction. The collective action problem then leads to under-provision of AML regulations on cryptocurrency ecosystem. Even more concerning, if AML regulation impose excessive burdens on businesses, countries will race to the bottom to offer more lenient regulation to attract cryptocurrency business back (Marian, 2019).

Thus, effective regulation of terrorism financing can only be achieved at a global level. One of the solutions is to set up a centralized coordinator. For example, the establishment of the Financial Action Task Force (FATF) is aimed at solving this collective action problem. It was created to address the overlapping jurisdictions and complexities associated with combating terrorist financing. The FATF functions as a provider of the public good that global AML regulation represents, much like a country serves as the provider of national defense. Looking ahead, the existing centralized AML regulatory framework need to be updated to keep pace with technological advancements.

8. Limitation and Further Study

8.1 Data Restriction

The reliability of the results is constrained by data limitations. For example, although this research utilizes panel data, there are only 19 countries included as units of analysis. Due to licensing issues, Auer et al. (2022) could only provide a portion of the dataset. Additionally, the regulation data is not comprehensive, as this research lacks information on regulatory activities after June 2019.

8.2 Robustness Check

The robustness check for this research did not perform well. While the two instrumental variables passed the underidentification test, weak identification test, and Sargan-Hansen test in simple regressions for total attacks and capital-intensive attacks, they only passed the Sargan-Hansen test when brutality was the dependent variable. Furthermore, these instruments did not perform adequately in the DID model either. This suggests that the explanatory variable may still suffer from endogeneity issues.

8.3 Further Study Possibilities

First, if funding permits, I will acquire the remaining data on monthly active users and monthly downloads of cryptocurrency applications for the other 76 countries. Having comprehensive data would help mitigate the issue of selection bias and provide more thorough insights into the relationship between cryptocurrency adoption and terrorism financing.

Second, I will use a staggered DID model for this research. This model does not require a proxy to represent the intensity of treatment; instead, it leverages the varying timings at which different units receive treatment to construct the DID analysis. As different countries introduced cryptocurrency regulations at different times, a staggered DID approach is well-suited and offers broader data coverage. However, some countries altered their stance on cryptocurrency within the study period, first imposing bans and later repealing them. Additionally, countries implement varying levels of regulation, ranging from hard bans to mere AML regulations, making it difficult to ensure consistency in treatment across all units.

Finally, this essay does not account for regulation trends after mid-2019 due to a lack of readily available data. In future research, I plan to follow the methods of Feinstein & Werbach (2021) to collect all relevant regulation news. A significant change of cryptocurrency market took place after the onset of COVID-19 (Jabotinsky & Sarel, 2022) and the war in Ukraine, and this research did not capture the global regulatory activity during such period. Additionally, applying other cutoff time points will be necessary to ensure the robustness of the study's findings.

9. Conclusion

This research presents a novel approach to evaluating the effectiveness of cryptocurrency regulation. It compiled a country-month level panel data for 19 countries from August 2015 to June 2021. By employing a DID model with a continuous treatment-cryptocurrency adoption-this research founds that the existing AML regulations on cryptocurrency have not significantly reduced the frequency of terrorist attacks, including those are capital-intensive. However, the period of globally coordinated regulation from December 2017 to June 2018 leads to a noticeable decrease in the brutality of attacks, an effect not observed with other isolated regulations. The results, however, are subject to further robustness check.

The explanations for insignificance are multi-faceted due to the complex causal link between AML regulation and the occurrence of attacks. The challenges may stem from the effectiveness of regulation, the degree of cryptocurrency engagement in terrorism financing, or the overall effectiveness of CTF efforts.

Furthermore, while international regulation is proved to be more effective, countries are under-incentivized to take action. DLT, as a common good, is non-excludable and rivalrous. The benefit of CTF, as a public good, is non-excludable and non-rivalrous. Positioned between these two dynamics, AML regulation places countries in a prisoners' dilemma, where they will ultimately choose non-cooperative solutions. A centralized coordinator is critical to ensure effective global cooperation.

Bibliography

Acharya, A. (2009). *Targeting Terrorist Financing: International Cooperation and New Regimes*. Routledge. https://doi.org/10.4324/9780203873717

Akcinaroglu, S., & Shi, M. (2023). Exploring the Impact of Cryptocurrency on Terrorism. *Terrorism and Political Violence*, *0*(0), 1–25. https://doi.org/10.1080/09546553.2023.2275057

Amiram, D., Jørgensen, B. N., & Rabetti, D. (2022). Coins for Bombs: The Predictive Ability of On-Chain Transfers for Terrorist Attacks. *Journal of Accounting Research*, *60*(2), 427–466. https://doi.org/10.1111/1475-679X.12430

Auer, R., & Claessens, S. (2018). *Regulating cryptocurrencies: Assessing market reactions*. https://www.bis.org/publ/qtrpdf/r_qt1809f.htm

Auer, R., Cornelli, G., Doerr, S., Frost, J., & Gambacorta, L. (2022). *Crypto trading and Bitcoin prices: Evidence from a new database of retail adoption*. https://www.bis.org/publ/work1049.htm

Bauer, K., & Levitt, M. (2020). Funding in Place: Local Financing Trends Behind Today's Global Terrorist Threat. *The International Centre for Counter-Terrorism – The Hague (ICCT) Evolutions in Counter-Terrorism*, *2*, 47–76.

Biersteker, T. J., Eckert, S. E., & Abuza, Z. (Eds.). (2008). *Countering the financing of terrorism*. Routledge.

Borri, N., & Shakhnov, K. (2020). Regulation spillovers across cryptocurrency markets. *Finance Research Letters*, *36*, 101333. https://doi.org/10.1016/j.frl.2019.101333

Brown, S. D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal*, *89*(4), 327–339. https://doi.org/10.1177/0032258X16658927

Callaway, B., Goodman-Bacon, A., & Sant'Anna, P. H. C. (2024). *Difference-in-differences with a Continuous Treatment* (Working Paper 32117). National Bureau of Economic Research. https://doi.org/10.3386/w32117

Chainalysis. (2023, June 27). *Terrorism Financing: Israel Seizes $1.7M in Crypto from Hezbollah*. https://www.chainalysis.com/blog/israel-nbctf-hezbollah-iran-quds-crypto-seizure/

Chainalysis. (2024, February). *The 2024 Crypto Crime Report*. https://go.chainalysis.com/crypto-crime-2024.html

Clunan, A. L. (2006). The Fight against Terrorist Financing. *Political Science Quarterly*, *121*(4), 569–596. https://doi.org/10.1002/j.1538-165X.2006.tb00582.x

Colella, F., Maskus, K., & Peri, A. (2024). *Unintended Consequences of Money-Laundering Regulations* (Working Paper 03/24). RF Berlin - CReAM Discussion Paper Series. https://www.econstor.eu/handle/10419/295718

Committee on, Payments and Market, & Infrastructures. (2015). *Digital currencies*. https://www.bis.org/cpmi/publ/d137.htm

Covert, A. (2011, June 17). There's A Virus That Will Steal All Your Bitcoins. *Gizmodo Australia*. https://gizmodo.com.au/2011/06/theres-a-virus-that-will-steal-all-your-bitcoins/

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR3026.html

Dostov, V., & Shust, P. (2014). Cryptocurrencies: An unconventional challenge to the AML/CFT regulators? *Journal of Financial Crime*, *21*(3), 249–263. https://doi.org/10.1108/JFC-06-2013-0043

Feinstein, B. D., & Werbach, K. (2021). The Impact of Cryptocurrency Regulation on Trading Markets. *Journal of Financial Regulation*, *7*(1), 48–99. https://doi.org/10.1093/jfr/fjab003

Freeman, M., & Ruehsen, M. (2013). Terrorism Financing Methods: An Overview. *Perspectives on Terrorism*, *7*(4), 5–26.

Fry, J., & Cheah, E.-T. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis*, *47*, 343–352. https://doi.org/10.1016/j.irfa.2016.02.008

Goldman, Z. K., Maruyama, E., Rosenberg, E., Saravalle, E., & Solomon-Strauss, J. (2017). *TERRORIST USE OF VIRTUAL CURRENCIES: Containing the Potential Threat*. Center for a New American Security. https://www.jstor.org/stable/resrep06423

Haffke, L., Fromberger, M., & Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: The shortcomings of the fifth AML Directive (EU) and how to address them. *Journal of Banking Regulation*, *21*(2), 125–138. https://doi.org/10.1057/s41261-019-00101-4

Haigner, S., Schneider, F., & Wakolbinger, F. (2012). *Combating Money Laundering and the Financing of Terrorism: A Survey* (Working Paper 65). Economics of Security Working Paper. https://www.econstor.eu/handle/10419/119391

Hampton, N., & Baig, Z. (2015). Ransomware: Emergence of the cyber-extortion menace. *Australian Information Security Management Conference*. https://doi.org/10.4225/75/57b69aa9d938b

Hasbi, A. H., & Mahzam, R. (2018). Cryptocurrencies: Potential For Terror Financing. *RSIS Commentaries (Nanyang Technological University)*, *75*. https://dr.ntu.edu.sg/handle/10356/89009

He, D., & Habermeier, K. F. (2016, January 20). *Virtual Currencies and Beyond: Initial Considerations*. IMF. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Virtual-Currencies-and-Beyond-Initial-Considerations-43618

Hougan, M., Kim, H., & Lerner, M. (2019). *Economic and Non-Economic Trading In Bitcoin: Exploring the Real Spot Market For The World's First Digital Commodity*.

Jabotinsky, H. Y., & Sarel, R. (2022). How Crisis Affects Crypto: Coronavirus as a Test Case. *Hastings Law Journal*, *74*(2), 433–488.

Karmakar, S., Demirer, R., & Gupta, R. (2021). Bitcoin mining activity and volatility dynamics in the power market. *Economics Letters*, *209*. https://doi.org/10.1016/j.econlet.2021.110111

Kiser, S. (2005). *Financing Terror: An Analysis and Simulation to Affect Al Qaeda's Financial Infrastructures*. RAND Corporation. https://www.rand.org/pubs/rgs_dissertations/RGSD185.html

Korotayev, A., Vaskin, I., & Tsirel, S. (2021). Economic Growth, Education, and Terrorism: A Re-Analysis. *Terrorism and Political Violence*, *33*(3), 572–595. https://doi.org/10.1080/09546553.2018.1559835

Lee, H., & Choi, K.-S. (2021). Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework. *Victims & Offenders*, *16*(3), 363–384. https://doi.org/10.1080/15564886.2020.1835764

Limodio, N. (2022). Terrorism Financing, Recruitment, and Attacks. *Econometrica*, *90*(4), 1711–1742. https://doi.org/10.3982/ECTA18530

Liu, M., Chen, H., & Yan, J. (2021). Detecting Roles of Money Laundering in Bitcoin Mixing Transactions: A Goal Modeling and Mining Framework. *Frontiers in Physics*, *9*. https://doi.org/10.3389/fphy.2021.665399

Majumder, A., Routh, M., & Singha, D. (2019). A Conceptual Study on the Emergence of Cryptocurrency Economy and Its Nexus with Terrorism Financing. In R. Chandra Das (Ed.), *The Impact of Global Terrorism on Economic and Political Development* (pp. 125–138). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78769-919-920191012

Marian, O. Y. (2019). *Blockchain Havens and the Need for Their Internationally-Coordinated Regulation* (SSRN Scholarly Paper 3357168). https://papers.ssrn.com/abstract=3357168

Miller, D., Mockel, P., & Myers, G. (2019, January). *Blockchain: Opportunities for Private Enterprises in Emerging Markets* [Text/HTML]. IFC. https://www.ifc.org/en/insights-reports/2019/blockchain-report

Nabilou, H. (2019). How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency. *International Journal of Law and Information Technology*, *27*(3), 266–291. https://doi.org/10.1093/ijlit/eaz008

Nunn, N., & Qian, N. (2011). The Potato's Contribution to Population and Urbanization: Evidence From A Historical Experiment*. *The Quarterly Journal of Economics*, *126*(2), 593–650. https://doi.org/10.1093/qje/qjr009

Ogus, A. I. (2004). *Regulation: Legal Form and Economic Theory*. Bloomsbury Publishing.

Roide, N. A. (2022). Fintech and Anti-Money Laundering Regulation: Implementing an International Regulatory Hierarchy Premised on Financial Innovation. *Texas A&M Law Review*, *9*(2), 465–495. https://doi.org/10.37419/LR.V9.I2.5

Sarel, R. (2021). Property Rights in Cryptocurrencies: A Law and Economics Perspective. *North Carolina Journal of Law & Technology*, *22*(3), 389.

Sarel, R., Jabotinsky, H. Y., & Klein, I. (2023). Globalize Me: Regulating Distributed Ledger Technology. *Vanderbilt Journal of Transnational Law*, *56*(2), 435–482.

Schneider, F. G. (2010). The (Hidden) Financial Flows of Terrorist and Organized Crime Organizations: A Literature Review and Some Preliminary Empirical Results. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1584191

Seo, J., Park, M., Oh, H., & Lee, K. (2018). Money Laundering in the Bitcoin Network: Perspective of Mixing Services. *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, 1403–1405. https://doi.org/10.1109/ICTC.2018.8539548

Sezgin, F. S., & Özdurak, C. (2023). Are Crypto Assets Connected to Real World Shocks? The Nexus Between Terrorist Attacks, Bitcoin and NFTs. *Journal of Economic Policy Researches*, *10*(1), Article 1. https://doi.org/10.26650/JEPR1127482

Shanaev, S., Sharma, S., Ghimire, B., & Shuraeva, A. (2020). Taming the blockchain beast? Regulatory implications for the cryptocurrency Market. *Research in International Business and Finance*, *51*, 101080. https://doi.org/10.1016/j.ribaf.2019.101080

Song, Y., Chen, B., & Wang, X.-Y. (2023). Cryptocurrency technology revolution: Are Bitcoin prices and terrorist attacks related? *Financial Innovation*, *9*(1), 29. https://doi.org/10.1186/s40854-022-00445-3

Taylor, R., Fritsch, E., Saylor, M., Liederbach, J., & Tafoya, W. (2018). *Cyber Crime and Cyber Terrorism*. Pearson.

United States Department of Justice. (2020a, March 13). *Long Island Woman Sentenced to 13 Years' Imprisonment for Providing Material Support to ISIS*. Office of Public Affairs. https://www.justice.gov/opa/pr/long-island-woman-sentenced-13-years-imprisonment-providing-material-support-isis

United States Department of Justice. (2020b, August 12). *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*. Office of Public Affairs. https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

Verdugo-Yepes, C. (2008). Enhancing International Cooperation in the Fight Against the Financing of Terrorism. *Journal of Global Change and Governance*, *1*(3).

Wang, H.-M., & Hsieh, M.-L. (2024). Cryptocurrency is new vogue: A reflection on money laundering prevention. *Security Journal*, *37*(1), 25–46. https://doi.org/10.1057/s41284-023-00366-5

Wang, S., & Zhu, X. (2021). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing. *Policing: A Journal of Policy and Practice*, *15*(4), 2329–2340. https://doi.org/10.1093/police/paab059

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism*, *39*(3), 195–206. https://doi.org/10.1080/1057610X.2015.1119546

Whyte, C. (2023). Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise. *Studies in Conflict & Terrorism*, *46*(7), 1126–1149. https://doi.org/10.1080/1057610X.2018.1531565

Wood, G. (2014). *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. *151*, 1–32. https://www.semanticscholar.org/paper/ETHEREUM%3A-A-SECURE-DECENTRALISED-GENERALISED-LEDGER-Wood/3c50bb6cc3f5417c3325a36ee190e24f0dc87257

Zhong, M. (2002). A faster single-term divisible electronic cash: ZCash. *Electronic Commerce Research and Applications*, *1*(3), 331–338. https://doi.org/10.1016/S1567-4223(02)00024-8